IntraCore 40240/40480-10G

Layer 3 Gigabit Stackable Ethernet Switch

User's Manual

IC40240-10G/IC40480-10G

(P/N 99-00837/99-00836)

User's Manual

Asante Networks

47709 Fremont Blvd., Fremont, CA 94538 USA

SALES

408-435-8388

TECHNICAL SUPPORT

408-435-8388: Worldwide

www.asante.com/support
support@asante.com

IntraCore 40240-10G Gigabit Ethernet Switch

- Stackable Layer 3 Switch
- 20 10/100/1000BASE-T (RJ-45) Ports,
- 4 Gigabit Combination Ports (RJ-45/SFP),
- 2 10-Gigabit Extender Module Slots,
- 2 Stacking Ports

IntraCore 40480-10G Gigabit Ethernet Switch

- Stackable Layer 3 Switch
- 44 10/100/1000BASE-T (RJ-45) Ports,
- 4 Gigabit Combination Ports (RJ-45/SFP),
- 2 10-Gigabit Extender Module Slots,
- 2 Stacking Ports

IC40240-10G (99-00837)
IC40480-10G (99-00836)

About This Manual

Purpose

This guide gives specific information on how to operate and use the management functions of the switch.

Audience

The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions

The following conventions are used throughout this guide to show information: **Note:** Emphasizes important information or calls your attention to related features or instructions. **Caution:** Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications

The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch: The *Installation Guide* Also, as part of the switch's software, there is an online web-based help that describes all management related features.

Revision History

This section summarizes the changes in each revision of this manual.

June 2009 Revision

This is the first release of this manual.

Contents

Section I: Getting Started

Section II: Switch Management

Section III: Command Line Interface

Section IV: Appendices

Tables

Figures

Chapter 1: Introduction

This switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

Key Features

Table 1-1 Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS Telnet – SSH SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X, MAC address filtering
Access Control Lists	Supports up to 256 ACLs, 96 MAC rules, 96 IP rules, and 96 IPv6 rules
DHCP Client, Relay and Server	Supported
DNS	Client and Proxy service
Port Configuration	Speed and duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 32 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Address Table	Up to 16K MAC addresses in the forwarding table, 1024 static MAC addresses; Up to 2K IPv4 and 1K IPv6 entries in the host table, 4K entries in the ARP cache; 256 IPv4 and 256 IPv6 entries in the IP routing table, 64 static IP routes; 32 IP interfaces
IP Version 4 and 6	Supports IPv4 and IPv6 addressing, management, and QoS
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames

Table 1-1 Key Features (Continued)

Feature	Description
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 256 using IEEE 802.1Q, port-based, protocol-based, or private VLANs
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
Qualify of Service	Supports Differentiated Services (DiffServ)
Router Redundancy	Router backup is provided with the Virtual Router Redundancy Protocol (VRRP)
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query

Description of Software Features

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Untagged (port-based), tagged, and protocol-based VLANs, plus support for automatic GVRP VLAN registration provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications. Some of the management features are briefly described below.

Configuration Backup and Restore – You can save the current configuration settings to a file on a TFTP server, and later download this file to restore the switch configuration settings.

Authentication – This switch authenticates management access via the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified via a remote authentication server (i.e., RADIUS or TACACS+). Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication server to verify the client’s right to access the network via an authentication server (i.e., RADIUS server).

Other authentication options include HTTPS for secure management access via the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can by used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

DHCP Server and DHCP Relay – A DHCP server is provided to assign IP addresses to host devices. Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.

Port Configuration – You can manually configure the speed and duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3-2005 (formerly IEEE 802.3ad) Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 32 trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

Store-and-Forward Switching – The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 2 MB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Algorithm – The switch supports these spanning tree protocols:

Spanning Tree Protocol (STP, IEEE 802.1D) – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

Virtual LANs – The switch supports up to 255 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned via GVRP, or ports can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN, except where a connection is explicitly defined via the switch’s routing service.

- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and allowing you to limit the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

Traffic Prioritization – This switch prioritizes each packet based on the required level of service, using eight priority queues with strict or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame’s Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

IP Routing – The switch provides Layer 3 IP routing. To maintain a high rate of throughput, the switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by this switch lets you easily link network segments or VLANs together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

RIP – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.

OSPF – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

Router Redundancy – The Virtual Router Redundancy Protocol (VRRP) uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of this protocol is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Address Resolution Protocol – The switch uses ARP and Proxy ARP to convert between IP addresses and MAC (i.e., hardware) addresses. This switch supports conventional ARP, which locates the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next. You can configure either static or dynamic entries in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination via the switch, which uses its own routing table to reach the destination on the other network.

Quality of Service – Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

System Defaults

The switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg." To reset the switch defaults, this file should be set as the startup configuration file (page 4-24).

The following table lists some of the basic system defaults.

Table 1-2 System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	auto
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)
Authentication	Privileged Exec Level	Username "admin" Password "admin"
	Normal Exec Level	Username "guest" Password "guest"
	Enable Privileged Exec from Normal Exec Level	Password "super"
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
SNMP	SNMP Agent	Enabled
	Community Strings	"public" (read only) "private" (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read only); private (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: All values based on IEEE 802.1w)
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled

Table 1-2 System Defaults (Continued)

Function	Parameter	Default
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	WRR
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	Management. VLAN	Any VLAN configured with an IP address
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled Relay: Disabled Server: Disabled
	DNS	Client/Proxy service: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPF	Disabled
Router Redundancy	VRRP	Disabled
Multicast Filtering	IGMP Snooping	Snooping: Enabled Querier: Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Enabled (but no server defined)
SNTP	Clock Synchronization	Disabled

Chapter 2: Initial Configuration

Connecting to the Switch

Configuration Options

The switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON (Groups 1, 2, 3, 9) and a web-based interface. A PC may also be connected directly to the switch for configuration and monitoring via a command line interface (CLI).

Note: An IPv4 address for this switch is obtained via DHCP by default. To change this address, see “Setting an IP Address” on page 2-7.

The switch’s HTTP web agent allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above. The switch’s web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the switch, or remotely by a Telnet connection over the network.

The switch’s management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the switch to be managed from any system in the network using network management software such as HP Openview. The switch’s web interface, CLI configuration program, and SNMP agent allow you to perform the following management functions:

- Set user names and passwords
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable/disable any port
- Set the speed/duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 255 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast traffic
- Configure router redundancy
- Configure IGMP multicast filtering
- Upload and download system firmware via TFTP
- Upload and download switch configuration files via TFTP

- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 6 static or LACP trunks per switch, up to 32 per stack
- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics
- Configure any stack unit through the same IP address

Required Connections

The switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch. A null-modem console cable is provided with the switch.

Note: When configuring a stack, connect to the console port on the Master unit.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the switch. You can use the console cable provided with this package, or use a null-modem cable that complies with the wiring assignments shown in the Installation Guide.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable to the RS-232 serial port on the switch.
3. Make sure the terminal emulation software is set as follows:
   - Select the appropriate serial port (COM port 1 or COM port 2).
   - Set to any of the following baud rates: 9600, 19200, 38400, 57600, 115200 (Note: Set to 9600 baud if want to view all the system initialization messages.).
   - Set the data format to 8 data bits, 1 stop bit, and no parity.
   - Set flow control to none.
   - Set the emulation mode to VT100.
   - When using HyperTerminal, select Terminal keys, not Windows keys.

Notes: **1.** Refer to “Line Commands” on page 23-17 for a complete description of console configuration options.

2. Once you have set up the terminal correctly, the console login screen will be displayed.

For a description of how to use the CLI, see “Using the Command Line Interface” on page 21-1. For a list of all the CLI commands and detailed information on using the CLI, refer to “Command Groups” on page 21-10.

Remote Connections

Prior to accessing the switch’s onboard agent via a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

An IPv4 address for this switch is obtained via DHCP by default. To manually configure this address or enable dynamic address assignment via DHCP or BOOTP, see “Setting an IP Address” on page 2-7.

Notes: **1.** This switch supports four concurrent Telnet/SSH sessions.

2. Each VLAN group can be assigned its own IP interface address (page 2-7). You can manage the stack via any IP interface in the stack. In other words, the Master unit does not have to include an active port member of a VLAN interface used for management access.

3. Any VLAN group can be assigned an IP interface address (page 2-7) for managing the stack. Also, note that the Master unit does not have to include an active port member in the VLAN interface used for management access.

After configuring the switch’s IP parameters, you can access the onboard configuration program from anywhere within the attached network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, Netscape 6.2 or above, or Mozilla Firefox 2.0.0.0 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, you must use SNMP-based network management software.

Stack Operations

Up to eight 24-port or 48-port Gigabit switches can be stacked together as described in the *Installation Guide*. One unit in the stack acts as the Master for configuration tasks and firmware upgrade. All of the other units function in Slave mode, but can automatically take over management of the stack if the Master unit fails.

To configure any unit in the stack, first verify the unit number from the front panel of the switch, and then select the appropriate unit number from the web or console management interface.

Selecting the Stack Master

Note the following points about unit numbering:

- When the stack is initially powered on, the Master unit is selected based on the following rules:
  - If the Master/Slave push button is depressed on only one unit in the stack, that unit will serve as the stack Master.

- If Master/Slave push button is depressed on more than one unit, the system will select the unit with the lowest MAC address from those with the push button depressed as the stack Master.
- If Master/Slave push button is not depressed on any unit, the system will select the unit with the lowest MAC address as the stack Master.

- When the stack is initially powered on, the Master unit is designated as unit 1 for a ring topology. For a line topology, the stack is simply numbered from top to bottom, with the first unit in the stack designated at unit 1. This unit identification number appears on the Stack Unit ID LED on the front panel of the switch. It can also be selected on the front panel graphic of the web interface, or from the CLI.
- If the Master unit fails and another unit takes over control of the stack, the unit numbering will not change.
- If a unit in the stack fails or is removed from the stack, the unit numbers will not change. This means that when you replace a unit in the stack, the original configuration for the failed unit will be restored to the replacement unit.
- If a unit is removed from the stack and later reattached to the stack, it will retain the original unit number obtained during stacking.
- If a unit is removed from the stack, and powered up as a stand-alone unit, it will also retain the original unit number obtained during stacking.

Selecting the Backup Unit

Once the Master unit finishes booting up, it continues to synchronize configuration information to all of the Slave units in the stack. If the Master unit fails or is powered off, a new master unit will be selected based on the election rules described in the preceding section. The backup unit elected to serve as the new stack Master will take control of the stack without any loss of configuration settings. To ensure a logical fail over to next unit down in the stack, place the Slave unit with the lowest MAC address directly beneath the Master unit in the stack.

Recovering from Stack Failure or Topology Change

When a link or unit in the stack fails, a trap message is sent and a failure event is logged. The stack will be rebooted after any system failure or topology change. It takes two to three minutes to for the stack to reboot. If the Master unit fails, the backup unit will take over operations as the new Master unit, reboot the stack, and then select another backup unit after the stack finishes rebooting. Also note that powering down a unit or inserting a new unit in the stack will cause the stack to reboot. If a unit is removed from the stack (due to a power down or failure) or a new unit added to the stack, the original unit IDs are not affected after rebooting, and a new unit is assigned the lowest available unit ID.

Broken Link for Line and Wrap-around Topologies

All units in the stack must be connected via stacking cable. You can connect the units in a simple cascade configuration from the top to the bottom unit. Using this kind of line topology, if any link or unit in the stack fails, the stack will be broken in two. The Stack Link LED on the unit that is no longer receiving traffic from the next unit up or down in the stack will begin flashing to indicate that the stack link is broken.

When the stack fails, a Master unit is selected from the two stack segments, either the unit with the Master button depressed, or the unit with the lowest MAC address if the Master button is not depressed on any unit. The stack reboots and resumes operations. However, note that the IP address will be the same for any common VLANs (with active port connections) that appear in both of the new stack segments. To resolve the conflicting IP addresses, you should manually replace the failed link or unit as soon as possible. If you are using a wrap-around stack topology, a single point of failure in the stack will not cause the stack to fail. It would take two or more points of failure to break the stack apart.

Note: If a stack breaks apart, the IP address will be the same for any common VLANs (with active port connections) that appear in both stack segments.

Resilient IP Interface for Management Access

The stack functions as one integral system for management and configuration purposes. You can therefore manage the stack through any IP interface configured on the stack. The Master unit does not even have to include an active port member in the VLAN interface used for management access. However, if the unit to which you normally connect for management access fails, and there are no active port members on the other units within this VLAN interface, then this IP address will no longer be available. To retain a constant IP address for management access across fail over events, you should include port members on several units within the primary VLAN used for stack management.

Resilient Configuration

If a unit in the stack fails, the unit numbers will not change. This means that when you replace a unit in the stack, the original configuration for the failed unit will be restored to the replacement unit. This applies to both the Master and Slave units.

Renumbering the Stack

The startup configuration file maps configuration settings to each switch in the stack based on the unit identification number. If the units are no longer numbered sequentially after several topology changes or failures, you can reset the unit numbers using the “Renumbering” command in the web interface or CLI. Just remember to save the new configuration settings to a startup configuration file prior to powering off the stack Master.

Ensuring Consistent Code is Used Across the Stack

Consistent Runtime Code in Each Switch – The main board runtime firmware version for each unit in the stack must be the same as the Master unit’s runtime firmware. After Auto-ID assignment is completed, the Master unit checks the image versions for consistency. If the firmware versions (i.e., runtime code) configured for bootup on any slave units are not the same as those on the Master Unit, the stack will operate in Special Stacking Mode in which all backup units are disabled as described below:

- The master unit starts normal operation mode in standalone mode.
- The master unit can see all units in the stack and maintain stack topology.
- None of the other units can function (all ports will be disabled).
- All user-initiated commands to configure the non-functioning units are dropped. The master unit, however, will be able to communicate the following information to the non-functioning units:
  - Image downloads
  - Stack topology information
  - System configuration information already stored on the master.

In Special Stacking mode, the master unit displays warning messages whenever you log into the system through the CLI that inform you that an image download is required.

You can use the CLI, web or SNMP to download the runtime image from a TFTP server to the master unit. The master unit stores the image as its “Next boot image” and downloads the image to those backup units that are running a different image version. For information on downloading firmware, see “Managing Firmware” on page 4-21 or “File Management Commands” on page 23-10.

Basic Configuration

Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the Privileged Exec level and allow you to only display information and use basic utilities. To fully configure the switch parameters, you must access the CLI at the Privileged Exec level.

Note: You can only access the console interface through the Master unit in the stack.

Access to both CLI levels are controlled by user names and passwords. The switch has a default user name and password for each level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate your console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the Username prompt, enter “admin.”
3. At the Password prompt, also enter “admin.” (The password characters are not displayed on the console screen.)

4. The session is opened and the CLI displays the “Console#” prompt indicating you have access at the Privileged Exec level.

Setting Passwords

Note: If this is your first time to log into the CLI program, you should define new passwords for both default user names using the “username” command, record them and put them in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the switch, set the passwords as follows:

1. Open the console interface with the default user name and password “admin” to access the Privileged Exec level.

2. Type “configure” and press <Enter>.

3. Type “username guest password 0 *password*,” for the Normal Exec level, where *password* is your new password. Press <Enter>.

4. Type “username admin password 0 *password*,” for the Privileged Exec level, where *password* is your new password. Press <Enter>.

Note: ‘0’ specifies a password in plain text, ‘7’ specifies a password in encrypted form.

```
Username: admin
Password:

 CLI session with the 24/48 L3 GE Switch is opened.
 To end the CLI session, enter [Exit].

Console#configure                                                22-2
Console(config)#username guest password 0 [password]             25-2
Console(config)#username admin password 0 [password]
Console(config)#
```

Setting an IP Address

You must establish IP address information for the stack to obtain management access through the network. This can be done in either of the following ways:

Manual — You have to input the information, including IP address and subnet mask. If your management station is not in the same IP subnet as the stack’s master unit, you will also need to specify the default gateway router.

Dynamic — The switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Manual Configuration

You can manually assign an IP address to the switch. You may also need to specify a default gateway that resides between this device and management stations that exist on another network segment (if routing is not enabled on this switch). Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Note: An IPv4 address for this switch is obtained via DHCP by default.

Assigning an IPv4 Address

Before you can assign an IP address to the switch, you must obtain the following information from your network administrator:

- IP address for the switch
- Network mask for this network
- Default gateway for the network

To assign an IPv4 address to the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ip address *ip-address netmask*,” where “ip-address” is the switch IP address and “netmask” is the network mask for the network. Press <Enter>.
3. Type “exit” to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the switch belongs, type “ip default-gateway *gateway*,” where “gateway” is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 1                                  27-1
Console(config-if)#ip address 192.168.1.5 255.255.255.0           41-3
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254                  41-4
Console(config)#
```

Assigning an IPv6 Address

There are several ways to manually configure IPv6 addresses. This section describes how to configure a “link local” address for connectivity within the local subnet only, and another option that allows you to specify a “global unicast” address by first configuring a network prefix for use on a multi-segment network, and then configuring the host address portion of the address.

An IPv6 prefix or address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields. For detailed information on the other ways to assign IPv6 addresses, see “Setting the Switch’s IP Address (IP Version 6)” on page 4-9.

Link Local Address — All link-local addresses must be configured with a prefix of FE80. Remember that this address type makes the switch accessible over IPv6 for all devices attached to the same local subnet only. Also, if the switch detects that the address you configured conflicts with that in use by another device on the subnet, it will stop using the address in question, and automatically generate a link local address that does not conflict with any other devices on the local subnet.

To configure an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. Type “ipv6 address” followed by up to 8 colon-separated 16-bit hexadecimal values for the *ipv6-address* similar to that shown in the example, followed by the “link-local” command parameter. Then press <Enter>.

```
Console(config)#interface vlan 1                                   27-1
Console(config-if)#ipv6 address FE80::260:3EFF:FE11:6700
 link-local                                                        41-9
Console(config-if)#end
Console#show ipv6 interface                                       41-14
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::260:3EFF:FE11:6700/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF11:6700/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Address for Multi-segment Network — Before you can assign an IPv6 address to the switch that will be used to connect to a multi-segment network, you must obtain the following information from your network administrator:

- Prefix for this network
- IP address for the switch
- Default gateway for the network

For most networks that encompass several different subnets, it’s easier to first define a network prefix, and then configure the host address for the switch. An IPv6 network prefix is composed of an IPv6-address and prefix length. The prefix length is the number of bits (from the left) of the prefix that form the network address, and is expressed as a decimal number. For example, all IPv6 address that start with the first byte of 73 (hexadecimal) could be expressed as 73:0:0:0:0:0:0:0/8 or 73::/8.

To generate an IPv6 global unicast address for the switch using a general network prefix, complete the following steps:

1. From the Global Configuration mode prompt, type “ipv6 general prefix *prefix-name ipv6-prefix/prefix-length*,” where the “prefix-name” is a label identifying the network segment, “ipv6-prefix” specifies the high-order bits of the network address, and “prefix length” indicates the actual number of bits used in the network prefix. Press <Enter>.

2. From the global configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

3. From the interface prompt, type “ipv6 address *prefix-name ipv6-address*/ *prefix-length*,” where “prefix-length” indicates the address bits used to form the network portion of the address. (The network address starts from the left of the general prefix and should encompass some of the ipv6-address bits.) The remaining bits are assigned to the host interface. Press <Enter>.

4. Type “exit” to return to the global configuration mode prompt. Press <Enter>.

5. To set the IP address of the IPv6 default gateway for the network to which the switch belongs, type “ipv6 default-gateway *gateway*,” where “gateway” is the IPv6 address of the default gateway. Press <Enter>.

```
Console(config)#ipv6 general-prefix rd 2001:DB8:2222::/48       41-8
Console(config)#interface vlan 1                                 27-1
Console(config-if)#ipv6 address rd 0:0:0:7272::72/64            41-9
Console(config-if)#exit
Console(config)ipv6 default-gateway 2001:DB8:2222:7272::254
 41-17
Console(config)end
Console#show ipv6 interface                                     41-14
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2001:DB8:2222:7272::72, subnet is 2001:DB8:2222:7272::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF72:64/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#show ipv6 default-gateway                               41-17
ipv6 default gateway:  2001:DB8:2222:7272::254
```

Dynamic Configuration

Obtaining an IPv4 Address

If you select the “bootp” or “dhcp” option, IP will be enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be sent periodically in an effort to obtain IP configuration information. BOOTP and DHCP values can include the IP address, subnet mask, and default gateway. If the DHCP/BOOTP server is slow to respond, you may need to use the “ip dhcp restart client” command to re-start broadcasting service requests.

If the “bootp” or “dhcp” option is saved to the startup-config file (step 6), then the switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
   - To obtain IP settings via DHCP, type “ip address dhcp” and press <Enter>.
   - To obtain IP settings via BOOTP, type “ip address bootp” and press <Enter>.
3. Type “end” to return to the Privileged Exec mode. Press <Enter>.
4. Type “ip dhcp restart client” to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings by typing the “show ip interface” command. Press <Enter>.
6. Then save your configuration changes by typing “copy running-config startup-config.” Enter the startup file name and press <Enter>.

```
Console(config)#interface vlan 1                                      27-1
Console(config-if)#ip address dhcp                                    41-3
Console(config-if)#end
Console#ip dhcp restart client                                        39-2
Console#show ip interface                                             41-5
 IP address and netmask: 192.168.1.54 255.255.255.0 on VLAN 1,
 and address mode: DHCP
Console#copy running-config startup-config                           23-11
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.
```

Obtaining an IPv6 Address

Link Local Address — There are several ways to dynamically configure IPv6 addresses. The simplest method is to automatically generate a “link local” address (identified by an address prefix of FE80). This address type makes the switch accessible over IPv6 for all devices attached to the same local subnet.

To generate an IPv6 link local address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.
2. Type “ipv6 enable” and press <Enter>.

```
Console(config)#interface vlan 1                                    27-1
Console(config-if)#ipv6 enable                                      41-7
Console(config-if)#end
Console#show ipv6 interface                                         41-5
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Address for Multi-segment Network — To generate an IPv6 address that can be used in a network containing more than one subnet, the switch can be configured to automatically generate a unique host address based on the local subnet address prefix received in router advertisement messages. (DHCP for IPv6 will also be supported in future software releases.)

To dynamically generate an IPv6 host address for the switch, complete the following steps:

1. From the Global Configuration mode prompt, type “interface vlan 1” to access the interface-configuration mode. Press <Enter>.

2. From the interface prompt, type “ipv6 address autoconfig” and press <Enter>.

```
Console(config)#interface vlan 1                                    27-1
Console(config-if)#ipv6 address autoconfig                         41-10
Console(config-if)#end
Console#show ipv6 interface                                        41-14
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::212:CFFF:FE0B:4600/64
Global unicast address(es):
  2005::212:CFFF:FE0B:4600, subnet is 2005:0:0:0::/64
  3FFE:501:FFFF:100:212:CFFF:FE0B:4600, subnet is
3FFE:501:FFFF:100::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF0B:4600/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Enabling SNMP Management Access

The switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications such as HP OpenView. You can configure the switch to (1) respond to SNMP requests or (2) generate SNMP traps.

When SNMP management stations send requests to the switch (either to return information or to set a parameter), the switch provides the requested data or sets the specified parameter. The switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, you must specify a community string. The switch provides a default MIB View (i.e., an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, you may assign new views to version 1 or 2c community strings that suit your specific security requirements (see page 5-17).

Community Strings (for SNMP version 1 and 2c clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the switch. You therefore need to assign community strings to specified users, and set the access level.

The default strings are:

- **public** - with read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - with read-write access. Authorized management stations are able to both retrieve and modify MIB objects.

To prevent unauthorized access to the switch from SNMP version 1 or 2c clients, it is recommended that you change the default community strings.

To configure a community string, complete the following steps:

1. From the Privileged Exec level global configuration mode prompt, type "snmp-server community *string mode*," where "string" is the community access string and "mode" is **rw** (read/write) or **ro** (read only). Press <Enter>. (Note that the default mode is read only.)

2. To remove an existing string, simply type "no snmp-server community *string*," where "string" is the community access string to remove. Press <Enter>.

```
Console(config)#snmp-server community admin rw                  24-3
Console(config)#snmp-server community private
Console(config)#
```

Note: If you do not intend to support access to SNMP version 1 and 2c clients, we recommend that you delete both of the default community strings. If there are no community strings, then SNMP management access from SNMP v1 and v2c clients is disabled.

Trap Receivers

You can also specify SNMP stations that are to receive traps from the switch. To configure a trap receiver, use the "snmp-server host" command. From the Privileged Exec level global configuration mode prompt, type:

"snmp-server host *host-address community-string*
[version {1 | 2c | 3 {auth | noauth | priv}}]"

where "host-address" is the IP address for the trap receiver, "community-string" specifies access rights for a version 1/2c host, or is the user name of a version 3 host, "version" indicates the SNMP client version, and "auth | noauth | priv" means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>. For a more detailed description of these parameters, see "snmp-server host" on page 24-5. The following example creates a trap host for each type of SNMP client.

```
Console(config)#snmp-server host 10.1.19.23 batman                   24-5
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, you need to first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group. The following example creates one view called “mib-2” that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/ write views to a group call “r&d” and specifies group authentication via MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included         24-10
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d          24-11
Console(config)#snmp-server user steve group r&d v3 auth md5
 greenpeace priv des56 einstien                                     24-14
Console(config)#
```

For a more detailed explanation on how to configure the switch for access from SNMP v3 clients, refer to “Simple Network Management Protocol” on page 5-1, or refer to the specific CLI commands for SNMP starting on page 24-1.

Managing System Files

The switch’s flash memory supports three types of system files that can be managed by the CLI program, web interface, or SNMP. The switch’s file system allows files to be uploaded and downloaded, copied, deleted, and set as a start-up file.

The three types of files are:

- **Configuration** — This file type stores system configuration information and is created when configuration settings are saved. Saved configuration files can be selected as a system start-up file or can be uploaded via TFTP to a server for backup. The file named “Factory_Default_Config.cfg” contains all the system default settings and cannot be deleted from the system. If the system is booted with the factory default settings, the master unit will also create a file named “startup1.cfg” that contains system settings for stack initialization, including information about the unit identifier, MAC address, and installed module type for each unit the stack. The configuration settings from the factory defaults configuration file are copied to this file, which is then used to boot the stack. See “Saving or Restoring Configuration Settings” on page 4-24 for more information.

- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the switch operations and provides the CLI and web management interfaces. See “Managing Firmware” on page 4-21 for more information.

- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).

Due to the size limit of the flash memory, the switch supports only two operation code files. However, you can have as many diagnostic code files and configuration files as available flash memory space allows. The switch has a total of 32 Mbytes of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. If you download directly to the running-config, the system will reboot, and the settings will have to be copied from the running-config to a permanent file.

Saving Configuration Settings

Configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save all your configuration changes in nonvolatile storage, you must copy the running configuration file to the start-up configuration file using the “copy” command.

New startup configuration files must have a name specified. File names on the switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

There can be more than one user-defined configuration file saved in the switch’s flash memory, but only one is designated as the “startup” file that is loaded when the switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config:**<*filename*> command.

The maximum number of saved configuration files depends on available flash memory, with each configuration file normally requiring less than 20 kbytes. The amount of available flash memory can be checked by using the **dir** command.

To save the current configuration settings, enter the following command:

1. From the Privileged Exec mode prompt, type “copy running-config startup-config” and press <Enter>.

2. Enter the name of the start-up file. Press <Enter>.

```
Console#copy running-config startup-config                       23-11
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

Section II: Switch Management

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser, and a brief example for the Command Line Interface.

Chapter 3: Configuring the Switch

Using the Web Interface

This switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0, Netscape 6.2, Mozilla Firefox 2.0.0.0, or more recent versions).

Note: You can also use the Command Line Interface (CLI) to manage the switch over a serial connection to the console port or via Telnet. For more information on using the CLI, refer to Chapter 21: “Overview of the Command Line Interface.”

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configure the switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See “Setting an IP Address” on page 2-7.)
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See “Setting Passwords” on page 2-7.)
3. After you enter a user name and password, you will have access to the system configuration program.

Notes:

1. You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

2. If you log into the web interface as guest (Normal Exec level), you can view the configuration settings or change the guest password. If you log in as “admin” (Privileged Exec level), you can change the settings on any page.

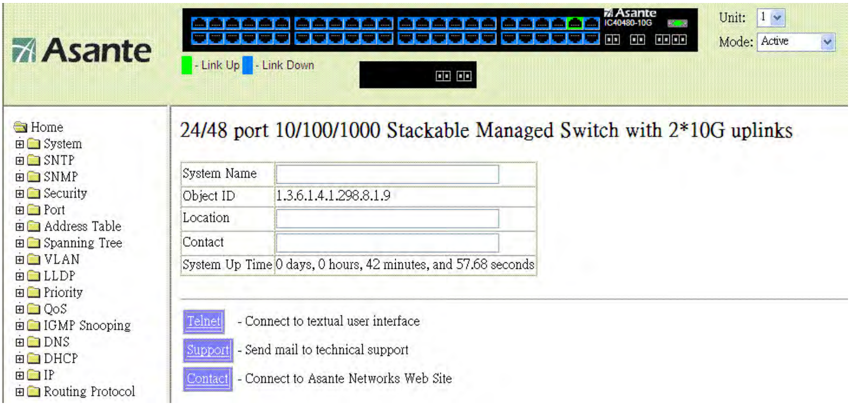
3. If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Algorithm, then you can set the switch port attached to your management station to fast forwarding (i.e., enable Admin Edge Port) to improve the switch’s response time to management commands issued through the web interface. See “Configuring Interface Settings” on page 10-13.

Navigating the Web Browser Interface

To access the web-browser interface you must first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name and password “admin” is used for the administrator.

Home Page

When your web browser connects with the switch’s web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.



Unit: 1
Mode: Active

24/48 port 10/100/1000 Stackable Managed Switch with 2*10G uplinks

System Name	
Object ID	1.3.6.1.4.1.298.8.1.9
Location	
Contact	
System Up Time	0 days, 0 hours, 42 minutes, and 57.68 seconds

Telnet - Connect to textual user interface
Support - Send mail to technical support
Contact - Connect to Asante Networks Web Site

Figure 3-1 Home Page

Note: The examples in this chapter are based on the IC40480-10G. Other than the number of fixed ports, there are no other differences between the IC40240-10G and IC40480-10G. The panel graphics for both switch types are shown on the following page.

Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes the web page configuration buttons.

Table 3-1 Web Page Configuration Buttons

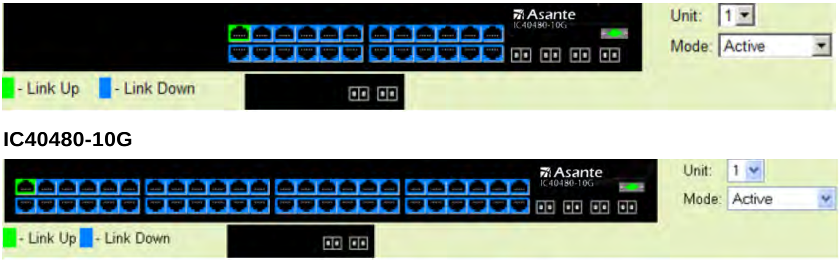
Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing Apply.
Help	Links directly to web help.

Notes: **1.** To ensure proper screen refresh, be sure that Internet Explorer is configured so that the setting “Check for newer versions of stored pages” reads “Every visit to the page”.
Internet Explorer 6.x and earlier: This option is available under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings”.
Internet Explorer 7.x: This option is available under “Tools / Internet Options / General / Browsing History / Settings / Temporary Internet Files”.

2. You may have to manually refresh the screen after making configuration changes by pressing the browser’s refresh button.

Panel Display

The web agent displays an image of the switch’s ports. The Mode can be set to display different information for the ports, including Active (i.e., up or down), Duplex (i.e., half or full duplex), or Flow Control (i.e., with or without flow control). Clicking on the image of a port opens the Port Configuration page as described on page 8-3.



IC40240-10G

🟩 - Link Up 🟦 - Link Down

Unit: 1

Mode: Active

IC40480-10G

🟩 - Link Up 🟦 - Link Down

Unit: 1

Mode: Active

Figure 3-2 Front Panel Indicators

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 3-2 Switch Main Menu

Menu	Description	Page
System		4-1
System Information	Provides basic system description, including contact information	4-1
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	4-3
Bridge Extension	Shows the bridge extension parameters	4-4
IP Configuration	Sets the IPv4 address for management access	4-5
IPv6 Configuration	Configures IPv6 interface addresses and static neighbors	4-9
IPv6 Configuration	Configures IPv6 interface address and protocol settings	4-9
IPv6 General Prefix	Configures IPv6 general prefix for network portion of addresses	4-15
IPv6 ND Neighbor	Configures IPv6 neighbor discover protocol and static neighbors	4-17
Jumbo Frames	Enables support for jumbo frames	4-21
File Management		4-21
Copy Operation	A lows the transfer and copying files	4-22
Delete	Allows deletion of files from the flash memory	4-22
Set Startup	Sets the startup file	4-22
Line		4-26
Console	Sets console port connection parameters	4-26
Telnet	Sets Telnet connection parameters	4-28
Log		4-30
Logs	Sends error messages to a logging process	4-33
System Logs	Stores and displays error messages	4-30
Remote Logs	Configures the logging of messages to a remote logging process	4-31
SMTP	Sends an SMTP client message to a participating server	4-33
Renumbering	Renumbers the units in the stack	4-35
Reset	Restarts the switch	4-36

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
SNTP	Simple Network Time Protocol	4-36
Current Time	Sets the time for the system clock	4-36
Configuration	Configures SNTP client settings, including a list of servers	4-37
Time Zone	Sets the local time zone for the system clock	4-39
Summer Time	Configures summer-time settings	4-40
SNMP	Simple Network Management Protocol	5-1
Configuration	Configures community strings and related trap functions	5-3
Agent Status	Enables or disables SNMP	5-2
SNMPv3		5-7
Engine ID	Sets the SNMP v3 engine ID	5-7
Remote Engine ID	Sets the SNMP v3 engine ID on a remote device	5-8
Users	Configures SNMP v3 users	5-9
Remote Users	Configures SNMP v3 users on a remote device	5-11
Groups	Configures SNMP v3 groups	5-13
Views	Configures SNMP v3 views	5-17
Security		6-1
User Accounts	Configures user names, passwords, and access levels	6-1
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	6-2
HTTPS Settings	Configures secure HTTP settings	6-5
SSH	Secure Shell	6-8
Settings	Configures Secure Shell server settings	6-14
Host-Key Settings	Generates the host key pair (public and private)	6-10
User Public-Key Settings	Imports and manages user RSA and DSA public keys	6-12
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	6-16
802.1X	Port authentication	6-18
Information	Displays global configuration settings	6-19
Configuration	Configures global configuration parameters	6-20
Port Configuration	Sets the authentication mode for individual ports	6-20
Statistics	Displays protocol statistics for the selected port	6-24
ACL	Access Control Lists	7-1
Configuration	Configures packet filtering based on IP or MAC addresses	7-1
Port Binding	Binds a port to the specified ACL	7-11

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
IP Filter	Configures IP addresses that are allowed management	6-26
Port	access	8-1
Port Information		8-1
Trunk Information	Displays port connection status	8-1
Port Configuration	Displays trunk connection status	8-3
Trunk Configuration	Configures port connection settings	8-3
Trunk Membership	Configures trunk connection settings	8-7
LACP	Specifies ports to group into static trunks	8-8
Configuration	Allows ports to dynamically join trunks	8-8
Aggregation Port	Configures parameters for link aggregation group members	8-10
Port Counters Information	Displays statistics for LACP protocol messages	8-13
Port Internal Information	Displays settings and operational state for the local side	8-14
Port Neighbors Information	Displays settings and operational state for the remote side	8-16
Port Broadcast Control	Sets the broadcast storm threshold for each port	8-17
Trunk Broadcast Control	Sets the broadcast storm threshold for each trunk	8-17
Mirror Port Configuration	Sets the source and target ports for mirroring	8-19
Rate Limit		8-20
Input Port Configuration	Sets the input rate limit for each port	8-20
Input Trunk Configuration	Sets the input rate limit for each trunk	8-20
Output Port Configuration	Sets the output rate limit for each port	8-20
Output Trunk Configuration	Sets the output rate limit for each trunk	8-20
Port Statistics	Lists Ethernet and RMON port statistics	8-22
Address Table		9-1
Static Addresses	Displays entries for interface, address or VLAN	9-1
Dynamic Addresses	Displays or edits static entries in the Address Table	9-2
Address Aging	Sets timeout for dynamically learned entries	9-4
Spanning Tree		10-1
STA	Spanning Tree Algorithm	
Information	Displays STA values used for the bridge	10-3
Configuration	Configures global bridge settings for STP, RSTP and MSTP	10-6
Port Information	Displays individual port settings for STA	10-10
Trunk Information	Displays individual trunk settings for STA	10-10

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
Port Configuration	Configures individual port settings for STA	10-13
Trunk Configuration	Configures individual trunk settings for STA	10-13
MSTP	Multiple Spanning Tree Algorithm	
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	10-16
Port Information	Displays port settings for a specified MST instance	10-19
Trunk Information	Displays trunk settings for a specified MST instance	10-19
Port Configuration	Configures port settings for a specified MST instance	10-20
Trunk Configuration	Configures trunk settings for a specified MST instance	10-20
VLAN		11-1
802.1Q VLAN		11-1
GVRP Status	Enables GVRP VLAN registration protocol	11-4
Basic Information	Displays information on the VLAN type supported by this switch	11-4
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	11-5
Static List	Used to create or remove VLAN groups	11-6
Static Table	Modifies the settings for an existing VLAN	11-7
Static Membership by Port	Configures membership type for interfaces, including tagged, untagged or forbidden	11-9
Port Configuration	Specifies default PVID and VLAN attributes	11-10
Trunk Configuration	Specifies default trunk VID and VLAN attributes	11-10
802.1Q Tunnel Configuration	Enables 802.1Q (QinQ) Tunneling	11-16
Tunnel Port Configuration	Sets the tunnel mode for an interface	11-17
Tunnel Trunk Configuration	Sets the tunnel mode for an interface	11-17
Private VLAN		11-18
Status	Enables or disables the private VLAN	11-19
Link Status	Configures the private VLAN	11-19
Protocol VLAN		11-20
Configuration	Creates a protocol group, specifying the supported protocols	11-20
Port Configuration	Maps a protocol group to a VLAN	11-21

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
LLDP	Link Layer Discovery Protocol	12-1
Configuration	Configures global LLDP timing parameters	12-1
Port Configuration	Configures parameters for individual ports	12-3
Trunk Configuration	Configures parameters for trunks	12-3
Local Information	Displays LLDP information about the local device	12-5
Remote Port Information	Displays LLDP information about a remote device connected to a port on this switch	12-8
Remote Trunk Information	Displays LLDP information about a remote device connected to a trunk on this switch	12-8
Remote Information Details	Displays detailed LLDP information about a remote device connected to this switch	12-9
Device Statistics	Displays LLDP statistics for all connected remote devices	12-11
Device Statistics Details	Displays LLDP statistics for remote devices on a selected port or trunk	12-13
Priority		13-1
Default Port Priority	Sets the default priority for each port	13-1
Default Trunk Priority	Sets the default priority for each trunk	13-1
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	13-3
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	13-5
Queue Scheduling	Configures Weighted Round Robin queueing	13-6
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	13-7
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	13-8
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	13-10
IP Port Priority Status	Globa ly enables or disables IP Port Priority	13-11
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	13-8
QoS	Quality of Service	14-1
DiffServ	Configure QoS classification criteria and service policies	14-1
Class Map	Creates a class map for a type of traffic	14-2
Policy Map	Creates a policy map for multiple interfaces	14-4
Service Policy	Applies a policy map defined to an ingress port	14-7

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
IGMP Snooping	Internet Group Management Protocol – Snooping	15-2
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	15-3
IGMP Immediate Leave	Configures immediate leave for multicast services no longer required	15-5
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	15-6
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	15-7
IP Multicast Registration Table	Displays all multicast groups active on this switch, including multicast IP addresses and VLAN ID	15-8
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	15-8
DNS	Domain Name Service	16-1
General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup	16-1
Static Host Table	Configures static entries for domain name to address mapping	16-3
Cache	Displays cache entries discovered by designated name servers	16-5
DHCP	Dynamic Host Configuration Protocol	17-1
Relay Configuration	Specifies DHCP relay servers; enables or disables relay service	17-1
Server	Configures DHCP server parameters	17-2
General	Enables DHCP server; configures excluded address range	17-3
Pool Configuration	Configures address pools for network groups or a specific host	17-4
IP Binding	Displays addresses currently bound to DHCP clients	17-9
VRRP	Virtual Router Redundancy Protocol	18-2
Group Configuration	Configures VRRP groups, including virtual interface address, advertisement interval, preemption, priority, and authentication	18-2
Global Statistics	Displays global statistics for VRRP protocol packet errors	18-7
Group Statistics	Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface	18-8
IP	Internet Protocol	19-1
General		19-4
Global Settings	Enables or disables routing, specifies the default gateway	19-4
Routing Interface	Configures the IP interface for the specified VLAN	19-5

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
ARP	Address Resolution Protocol	19-8
General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	19-9
Static Addresses	Statically maps a physical address to an IP address	19-11
Dynamic Addresses	Shows dynamically learned entries in the IP routing table	19-12
Other Addresses	Shows internal addresses used by the switch	19-13
Statistics	Shows statistics on ARP requests sent and received	19-14
Statistics		19-16
IP	Shows statistics for IP traffic, including the amount of traffic, address errors, routing, fragmentation and reassembly	19-16
ICMP	Shows statistics for ICMP traffic, including the amount of traffic, protocol errors, and the number of echoes, timestamps, and address masks	19-17
UDP	Shows statistics for UDP, including the amount of traffic and errors	19-19
TCP	Shows statistics for TCP, including the amount of traffic and TCP connection activity	19-20
Routing		19-21
Static Routes	Configures and display static routing entries	19-21
Routing Table	Shows all routing entries, including local, static and dynamic routes	19-22
Routing Protocol		20-1
RIP	Routing Information Protocol	20-2
General Settings	Enables or disables RIP, sets the global RIP version and timer values	20-3
Network Addresses	Configures the network interfaces that will use RIP	20-5
Interface Settings	Configures RIP parameters for each interface, including send and receive versions, message loopback prevention, and authentication	20-6
Redistribute Configuration	Imports external routing information from other routing domains into the autonomous system	20-9
Statistics	Displays general information on update time, route changes and number of queries, as well as a list of statistics for known interfaces and neighbors	20-11

Table 3-2 Switch Main Menu (Continued)

Menu	Description	Page
OSPF	Open Shortest Path First	20-14
General Configuration	Enables or disables OSPF; also configures the Router ID and various other global settings	20-15
Area Configuration	Specifies rules for importing routes into each area	20-19
Area Range Configuration	Configures route summaries to advertise at an area boundary	20-23
Interface Configuration	Shows area ID and designated router; also configures OSPF protocol settings and authentication for each interface	20-25
Virtual Link Configuration	Configures a virtual link through a transit area to the backbone	20-29
Network Area Address Configuration	Defines OSPF areas and associated interfaces	20-31
Summary Address Configuration	Aggregates routes learned from other protocols for advertising into other autonomous systems	20-33
Redistribute Configuration	Redistributes routes from one routing domain to another	20-35
NSSA Settings	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	20-36
Link State Database Information	Shows information about different OSPF Link State Advertisements (LSAs) stored in this router’s database	20-38
Border Router Information	Displays routing table entries for area border routers and autonomous system boundary routers	20-40
Neighbor Information	Displays information about neighboring routers on each interface within an OSPF area	20-41

Chapter 4: Basic Management Tasks

This chapter describes the basic functions required to set up management access to the switch, display or upgrade operating software, or reset the system.

Displaying System Information

You can easily identify the system by displaying the device name, location and contact information.

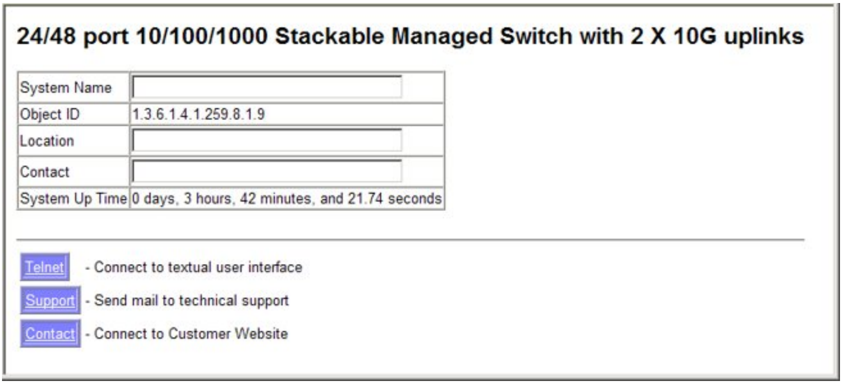
Field Attributes

- **System Name** – Name assigned to the switch system.
- **Object ID** – MIB II object ID for switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **System Description** – Brief description of device type.
- **MAC Address** – The physical layer address for this switch.
- **Web Server** – Shows if management access via HTTP is enabled.
- **Web Server Port** – Shows the TCP port number used by the web interface.
- **Web Secure Server** – Shows if management access via HTTPS is enabled.
- **Web Secure Server Port** – Shows the TCP port used by the HTTPS interface.
- **Telnet Server** – Shows if management access via Telnet is enabled.
- **Telnet Server Port** – Shows the TCP port used by the Telnet interface.
- **Authentication Login** – Shows the user login authentication sequence.
- **Jumbo Frame** – Shows if jumbo frames are enabled.
- **Jumbo Frame Size** – Configured size of jumbo frame.
- **POST Result** – Shows results of the power-on self-test

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface via Telnet.)



24/48 port 10/100/1000 Stackable Managed Switch with 2 X 10G uplinks

System Name	
Object ID	1.3.6.1.4.1.259.8.1.9
Location	
Contact	
System Up Time	0 days, 3 hours, 42 minutes, and 21.74 seconds

Telnet - Connect to textual user interface

Support - Send mail to technical support

Contact - Connect to Customer Website

Figure 4-1 System Information

CLI – Specify the hostname, location and contact information.

```
Console(config)#hostname R&D 5                                              23-1
Console(config)#snmp-server location WC 9                                   24-4
Console(config)#snmp-server contact Ted                                     24-4
Console(config)#exit
Console#show  system                                                        23-7
System Description: 24/48 port 10/100/1000 Stackable Managed Switch with
 2 X 10G   uplinks
System OID String: 1.3.6.1.4.1.259.8.1.9
System Information
 System Up Time:               0 days, 1 hours, 28 minutes, and 0.51 seconds
 System Name:               R&D 5
 System Location:           WC 9
 System Contact:            Ted
 MAC Address (Unit1):        00-20-1A-DF-9C-A0
 MAC Address (Unit2):        00-20-1A-DF-9E-C0
 Web Server:                Enabled
 Web Server Port:           80
 Web Secure Server:         Enabled
 Web Secure Server Port:   443
 Telnet Server:             Enable
 Telnet Server Port:        23
 Authentication Login:       Local RADIUS None
 Jumbo Frame:               Disabled
 Jumbo Frame Size:          1522
 POST Result:
DUMMY Test 1 ................. PASS
DRAM Test .................... PASS
Timer Test ................... PASS
PCI Device 1 Test ............ PASS
I2C Bus Initialization ....... PASS
Fan Speed Test ............... PASS

Done All Pass.
Console#
```

Displaying Switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – The serial number of the switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Internal Power Status** – Displays the status of the internal power supply.

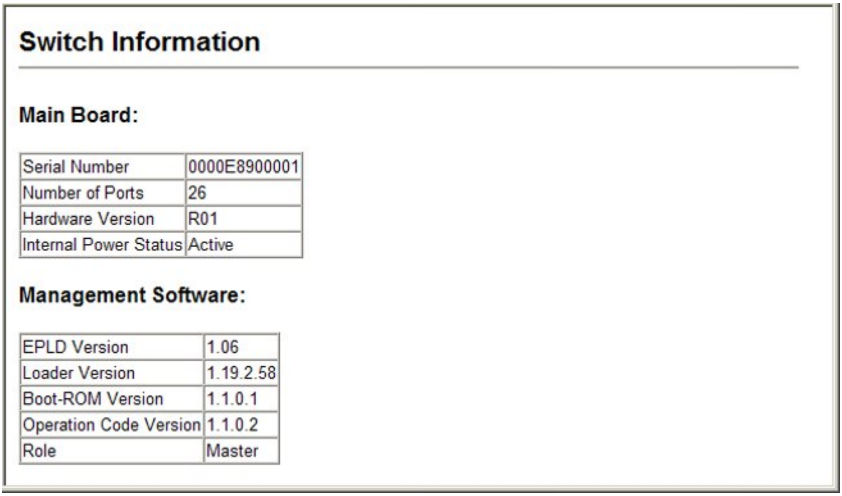
Management Software

- **EPLD Version** – Version number of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that this switch is operating as Master or Slave.

These additional parameters are displayed for the CLI.

- **Unit ID** – Unit number in stack.
- **Redundant Power Status** – Displays the status of the redundant power supply.

Web – Click System, Switch Information.



Switch Information

Main Board:

Serial Number	0000E8900001
Number of Ports	26
Hardware Version	R01
Internal Power Status	Active

Management Software:

EPLD Version	1.06
Loader Version	1.19.2.58
Boot-ROM Version	1.1.0.1
Operation Code Version	1.1.0.2
Role	Master

Figure 4-2 Switch Information

CLI – Use the following command to display version information.

```
Console#show version                                                    23-8
Unit 1
 Serial Number:            0000E8900001
 Hardware Version:         R01
 EPLD Version:             1.06
 Number of Ports:          26
 Main Power Status:        Up
 Redundant Power Status:   Not present

Agent (Master)
 Unit ID:                  1
 Loader Version:           1.19.2.58
 Boot ROM Version:         1.1.0.1
 Operation Code Version:   1.1.0.2

Console#
```

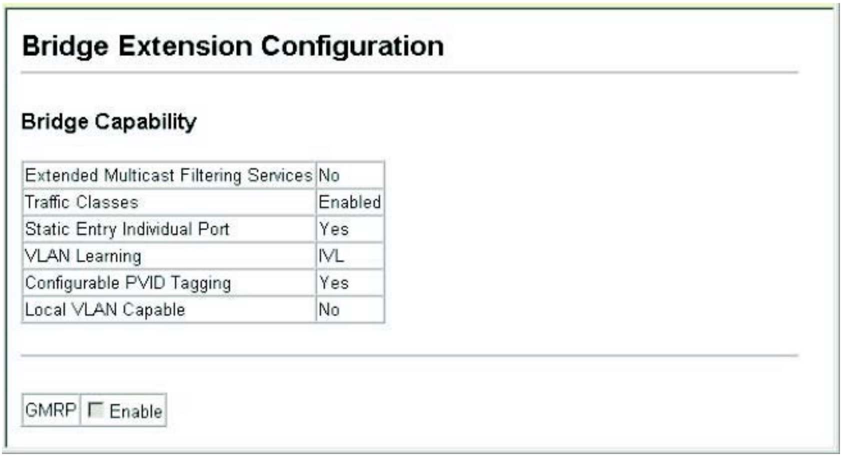
Displaying Bridge Extension Capabilities

The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. You can access these extensions to display default settings for the key variables.

Field Attributes

- **Extended Multicast Filtering Services** – This switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – This switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service” on page 13-1.)
- **Static Entry Individual Port** – This switch allows static filtering for unicast and multicast addresses. (Refer to “Setting Static Addresses” on page 9-1.)
- **VLAN Learning** – This switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – This switch allows you to override the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port. (Refer to “VLAN Configuration” on page 11-1.)
- **Local VLAN Capable** – This switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. This switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.



Bridge Extension Configuration

Bridge Capability

Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

GMRP □ Enable

Figure 4-3 Displaying Bridge Extension Configuration

CLI – Enter the following command.

```
Console#show bridge-ext                                                 34-2
 Max support VLAN numbers:                 4096
 Max support VLAN ID:                      4093
 Extended multicast filtering services:  No
 Static entry individual port:             Yes
 VLAN  learning:                           IVL
 Configurable PVID tagging:                Yes
 Local VLAN capable:                       No
 Traffic classes:                          Enabled
 Global GVRP status:                       Disabled
 GMRP:                                     Disabled
Console#
```

Setting the Switch's IP Address (IP Version 4)

This section describes how to configure an initial IPv4 interface for management access over the network. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv6 address, see "Setting the Switch's IP Address (IP Version 6)" on page 4-9.

The IPv4 address for this stack is obtained via DHCP by default. To manually configure an address, you need to change the stack's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the stack and management stations that exist on another network segment (if routing is not enabled on this stack).

You can manually configure a specific IP address, or direct the device to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the CLI program.

Command Usage

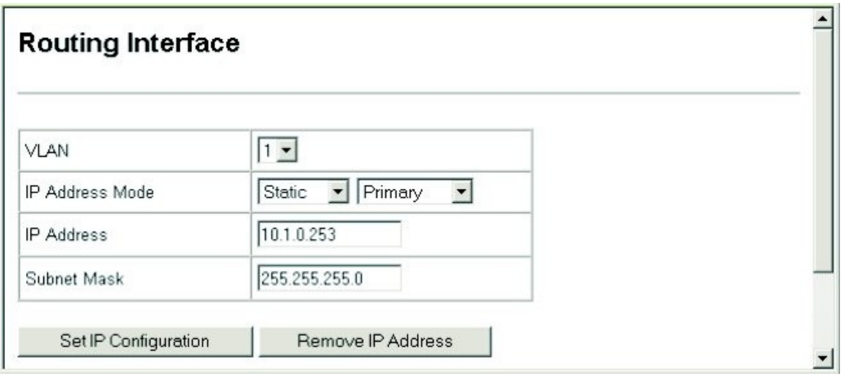
- This section describes how to configure a single local interface for initial access to the stack. To configure multiple IP interfaces on this stack, you must set up an IP interface for each VLAN (page 19-4).
- To enable routing between the different interfaces on this stack, you must enable IP routing (page 19-4).
- To enable routing between the interfaces defined on this stack and external network interfaces, you must configure static routes (page 19-21) or use dynamic routing; i.e., either RIP or OSPF (page 20-2 and page 20-14, respectively).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 19-5), static routes (page 19-21), and then dynamic routing.

Command Attributes

- **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the stack are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IP Address Mode** – Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)
- **IP Address** – Address of the VLAN to which the management station is attached. (Note that you can manage the stack through any configured IP interface.) Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
  (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Gateway IP Address** – IP address of the gateway router between the stack and management stations that exist on other network segments. (Default: 0.0.0.0)
- **MAC Address** – The physical layer address for this switch.

Manual Configuration

Web – Click IP, General, Routing Interface. Select the VLAN through which the management station is attached, set the IP Address Mode to "Static," and specify a "Primary" interface. Enter the IP address, and subnet mask, then click Apply.

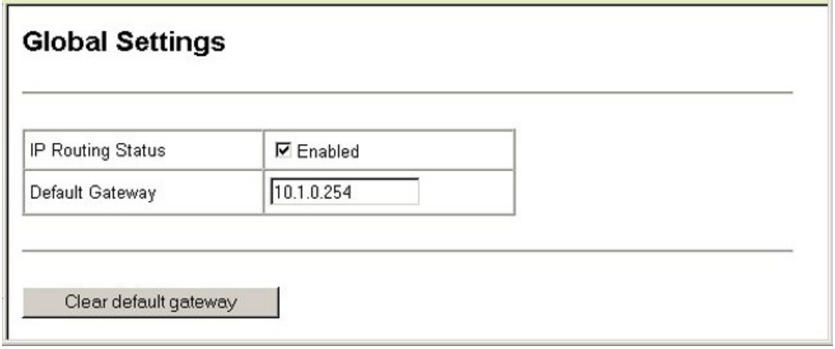


Routing Interface

VLAN	1
IP Address Mode	Static, Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0

Figure 4-4 IPv4 Interface Configuration - Manual

Click IP, Global Setting. If this stack and management stations exist on other network segments, then specify the default gateway, and click Apply.



Global Settings

IP Routing Status	☑ Enabled
Default Gateway	10.1.0.254

Figure 4-5 Default Gateway

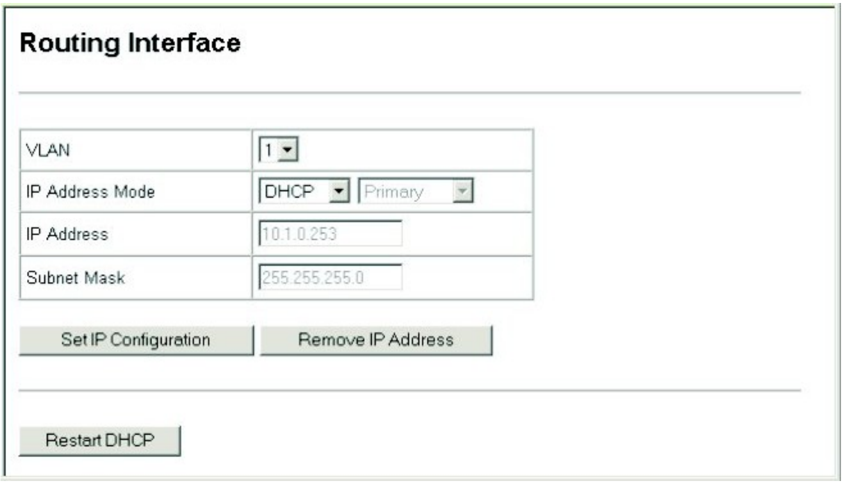
CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1                                        27-1
Console(config-if)#ip address 10.1.0.253 255.255.255.0                  41-3
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254                           41-4
Console(config)#
```

Using DHCP/BOOTP

If your network provides DHCP/BOOTP services, you can configure the stack to be dynamically configured by these services.

Web – Click IP, General, Routing Interface. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save your changes. Then click Restart DHCP to immediately request a new address. Note that the stack will also broadcast a request for IP configuration settings on each power reset.



Routing Interface

VLAN	1
IP Address Mode	DHCP, Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0

Figure 4-6 IPv4 Interface Configuration - DHCP

Note: If you lose your management connection, make a console connection to the Master unit and enter “show ip interface” to determine the new stack address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the “ip dhcp restart client” command.

```
Console#config
Console(config)#interface vlan 1                                        27-1
Console(config-if)#ip address dhcp                                      41-3
Console(config-if)#end
Console#ip dhcp restart client                                          39-2
Console#show ip interface                                               41-5

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.1.253, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Renewing DCHP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the stack is moved to another network segment, you will lose management access to the stack. In this case, you can reboot the stack or submit a client request to restart DHCP service via the CLI.

Web – If the address assigned by DHCP is no longer functioning, you will not be able to renew the IP settings via the web interface. You can only restart DHCP service via the web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```
Console#ip dhcp restart client                                   39-2
Console#
```

Setting the Switch’s IP Address (IP Version 6)

This section describes how to configure an initial IPv6 interface for management access over the network. This switch supports both IPv4 and IPv6, and can be managed through either of these address types. For information on configuring the switch with an IPv4 address, see “Setting the Switch’s IP Address (IP Version 4)” on page 4-5.

Configuring an IPv6 Address

IPv6 includes two distinct address types – link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address. Both link-local and global unicast address types can either be manually configured or dynamically assigned.

Command Usage

- This section describes how to configure a single local interface for initial access to the stack. To configure multiple IP interfaces on this stack, you must set up an IP interface for each VLAN (page 19-4).
- To enable routing between the different interfaces on this stack, you must enable IP routing (page 19-4).
- To enable routing between the interfaces defined on this stack and external network interfaces, you must configure static routes (page 19-21) or use dynamic routing; i.e., either RIP or OSPF (page 20-2 and 20-14, respectively).
- The precedence for configuring IP interfaces is the IP / General / Routing Interface menu (page 19-5), static routes (page 19-21), and then dynamic routing.
- All IPv6 addresses must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- The switch must always be configured with a link-local address. Therefore any configuration process that enables IPv6 functionality, or assigns a global unicast address to the switch, will also automatically generate a link-local unicast address. The prefix length for a link-local address is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the interface identifier (i.e., the physical MAC address). Alternatively, you can manually configure the link-local address by entering the full address with the network prefix FE80.
- To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:
  - The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address.
  - It can be manually configured by specifying the entire network prefix and prefix length, and using the EUI-64 form of the interface identifier to automatically create the low-order 64 bits in the host portion of the address.
  - You can also manually configure the global unicast address by entering the full address and prefix length.
  - Or you can include a general prefix for the network portion of the address (as described under “Configuring an IPv6 General Network Prefix” on page 4-15). When using this method, remember that the prefix length specified on the IPv6 Configuration page must include both the length of the general prefix and any contiguous bits (from the left of the specified address) that are added to the general prefix to form the extended network portion of the address.
- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- If a duplicate link-local address is detected on the local segment, this interface is disabled and a warning message displayed on the console. If a duplicate global unicast address is detected on the network, the address is disabled on this interface and a warning message displayed on the console.

Command Attributes

- **VLAN** – ID of the configured VLAN (1-4093). By default, all ports on the stack are members of VLAN 1. However, the management station can be attached to a port belonging to any VLAN, as long as that VLAN has been assigned an IP address.
- **IPv6 Address Processing** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.
- **IPv6 Interface Status** – Shows if IPv6 interface address configuration state is stable (Enabled) or unstable (Stale).
- **IPv6 Default Gateway** – Sets the IPv6 address of the default next hop router to use when no other routing information is known about an IPv6 address.
  - The specified gateway is only valid if routing is disabled using the IP / General / Global Settings screen (see page 19-4) or no other routing information is known

about the target address. If IP routing is disabled, you must define a gateway if the target device is located in a different subnet.

  - If routing is enabled, you can still define a static route using the IP / Routing / Static Routes screen (see page 19-21) to ensure that traffic to the designated address or subnet passes through a preferred gateway.
  - An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

- **IPv6 MTU** – Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. (Range: 1280-65535 bytes, Default: 1500 bytes)
  - If a non-default value is configured, an MTU option is included in the router advertisements sent from this device. This option is provided to ensure that all nodes on a link use the same MTU value in cases where the link MTU is not otherwise well known.
  - IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
  - All devices on the same physical medium must use the same MTU in order to operate correctly.
  - IPv6 must be enabled on an interface before the MTU can be set.

IPv6 Address Configuration

Configuration Mode – Selects Auto Configuration or Manual Configuration.

- **Auto Configuration** – Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier (i.e., the switch’s MAC address).
  - If the router advertisements have the “other stateful configuration” flag set, the switch will attempt to acquire other non-address configuration information (such as a default gateway) from a DHCP for IPv6 server.
- **Manual Configuration** – Enables IPv6 on an interface. Note that when an explicit address is assigned to an interface, IPv6 is automatically enabled, and cannot be disabled until all assigned addresses have been removed.
  - **IPv6 Address** – An IPv6 address can be configured in any of these ways:
    - A link-local address can be manually configured by specifying the entire address in the IPv6 Address field, and selecting the Address Type “Link Local.” The network prefix length is fixed at 64 bits and cannot be changed.
    - A global unicast address can be configured by specifying the network prefix and the length of the prefix (in the IPv6 Address field), and then selecting the Address Type “EUI-64” to automatically create the host portion of the address in the low order 64 bits based on the modified EUI-64 interface identifier.
    - A global unicast address can be manually configured by specifying the full address and network prefix length (in the IP Address field), and selecting the Address Type “Others.”

- A global unicast address can also be set by selecting a preconfigured general prefix for the network portion of the address from the Based on General Prefix scroll-down list and marking the check box next to this field to enable your choice (see “Configuring an IPv6 General Network Prefix” on page 4-15), and then specifying the address (in the IPv6 Address field) and the full network prefix length (e.g., /64 appended to the end of the specified address) which includes the general prefix and any contiguous bits starting at the left of the address that are appended to the network prefix.

Note About Prefix Length – To specify the prefix length, enter a forward slash followed by a decimal value indicating how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address).

When used with a general network prefix to configure a global unicast address, this length includes both that specified by the general prefix and any contiguous prefix bits (starting at the left of the specified address) that exceed the length of the general prefix. If the prefix length specified by this parameter is shorter than the general prefix, then the length of the general prefix takes precedence.

- **Based on General Prefix** – Defines a general prefix for the network segment of the address (see “Configuring an IPv6 General Network Prefix” on page 4-15).

  When configuring a global unicast address based on a general network prefix, the prefix length includes both that specified by the general prefix and any number of subsequent prefix bits that exceed the length of the general prefix. Therefore, depending on the specified prefix length, some of the address bits entered in the IPv6 Address field may be appended to the general prefix. However, if the prefix length is shorter than the general prefix, then the length of the general prefix takes precedence, and some of the address bits entered in the IPv6 Address field will be ignored.

- **Address Type** – Defines the address type configured for this interface.
  - **Link Local** – Configures an IPv6 link-local address.
    - The address prefix must be FE80.
    - You can configure only one link-local address per interface.
    - The specified address replaces a link-local address that was automatically generated for the interface.
  - **EUI-64** (Extended Universal Identifier) – Configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits.
    - When using EUI-64 format for the low-order 64 bits in the host portion of the address, the value entered in the IPv6 Address field includes the network portion of the address, and the prefix length indicates how many contiguous bits (starting at the left) of the address comprise the prefix (i.e., the network portion of the address). Note that the value specified in the IPv6 Address field may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the bits used in the network portion of the address will take precedence over the interface identifier.
    - IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device’s MAC address. The EUI-64

specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the MAC address.

For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., organizationally unique identifier, or company identifier) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

- **Others** – System will automatically detect the address type according to the address/prefix entered in the IPv6 Address field.

Current Address Table

- **IPv6 Address** – IPv6 address assigned to this interface.

  In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively.

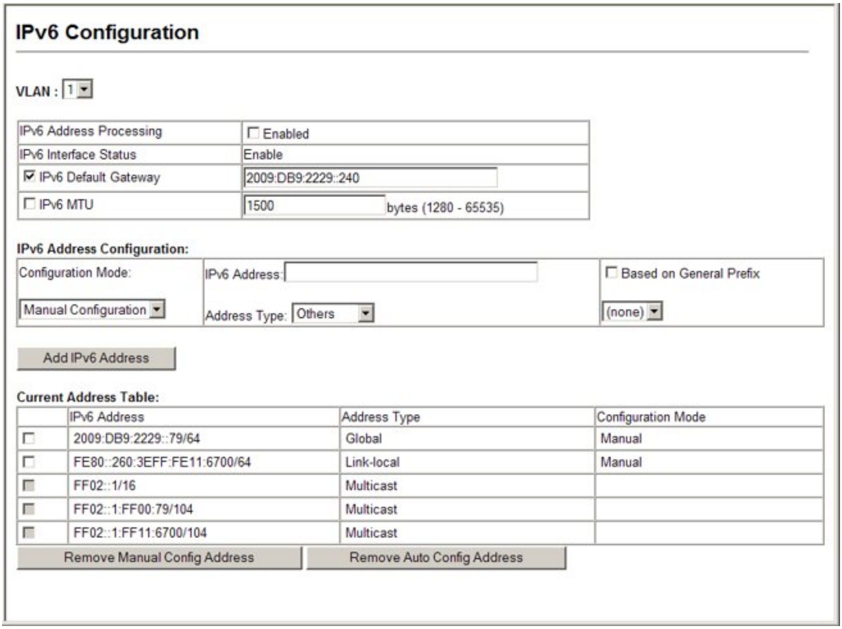
  FF01::1/16 is the transient node-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The node-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below.

  A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.

  Note that the solicited-node multicast address (link-local scope FF02) is used to resolve the MAC addresses for neighbor nodes since IPv6 does not support the broadcast method used by the Address Resolution Protocol in IPv4.

- **Address Type** – Global, Link-local or Multicast.
- **Configuration Mode** – Shows if address is set manually or auto configured.

Web – Click System, IPv6 Configuration, IPv6 Configuration. Set the IPv6 default gateway, specify the VLAN to configure, enable IPv6, and set the MTU. Then enter a global unicast or link-local address and click Add IPv6 Address.



IPv6 Configuration

VLAN : 1

IPv6 Address Processing	□ Enabled
IPv6 Interface Status	Enable
☑ IPv6 Default Gateway	2009:DB9:2229::240
□ IPv6 MTU	1500 bytes (1280 - 65535)

IPv6 Address Configuration:

Configuration Mode: Manual Configuration	IPv6 Address: Address Type: Others	□ Based on General Prefix (none)

Current Address Table:

	IPv6 Address	Address Type	Configuration Mode
□	2009:DB9:2229::79/64	Global	Manual
□	FE80::260:3EFF:FE11:6700/64	Link-local	Manual
□	FF02::1/16	Multicast	
□	FF02::1:FF00:79/104	Multicast	
□	FF02::1:FF11:6700/104	Multicast	

Figure 4-7 IPv6 Interface Configuration

CLI – This example configures an IPv6 gateway, specifies the management interface, configures a global unicast address, and then sets the MTU.

```
Console#config
Console(config)#ipv6 default-gateway 2009:DB9:2229::240             41-17
Console(config)#ipv6 general-prefix rd 2009:DB9:2229::/48            41-8
Console(config)#interface vlan 1                                     27-1
Console(config-if)#ipv6 address rd 7279::79/64                       41-9
Console(config-if)#ipv6 mtu 1280                                    41-18
Console(config-if)#ipv6 enable                                       41-7
Console(config-if)#end
Console#show ipv6 default-gateway                                   41-17
ipv6 default gateway:  2009:DB9:2229::240
Console#show ipv6 interface                                         41-14
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF11:4321/104
MTU is 1280 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#show ipv6 mtu                                               41-19
MTU      Since    Destination Address
1400     00:04:21  5000:1::3
1280      00:04:50   FE80::203:A0FF:FED6:141D
Console#
```

Configuring an IPv6 General Network Prefix

The IPv6 General Prefix page is used to configure general prefixes that are subsequently used on the IPv6 Configuration web page (see page 4-9) to specify the network address portion of an interface address.

Command Usage

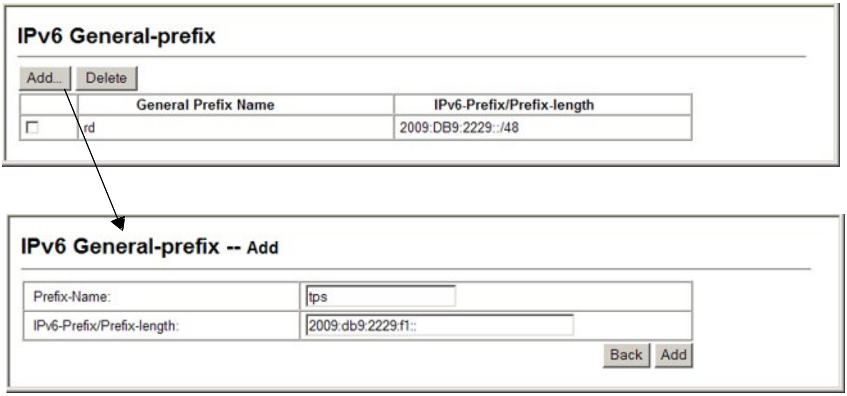
- Prefixes may contain zero-value fields or end in zeros.
- A general prefix holds a short prefix that indicates the high-order bits used in the network portion of the address. Longer, more specific, prefixes can be based on the general prefix to specify any number of subnets. When the general prefix is changed, all of the more specific prefixes based on this prefix will also change.

Command Attributes

- **General Prefix Name** – The label assigned to the general prefix.
- **IPv6-Prefix/Prefix-length** – The high-order bits of the network address segment assigned to the general prefix. The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Follow the prefix by a forward slash and a decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Web – Click System, IPv6 Configuration, IPv6 General Prefix. Click Add to open the editing fields for a prefix entry. Enter a name for the general prefix, the value for the general prefix, and the prefix length. Then click Add to enable the entry.



IPv6 General-prefix

	General Prefix Name	IPv6-Prefix/Prefix-length
□	rd	2009:DB9:2229::/48

IPv6 General-prefix -- Add

Prefix-Name:	tps
IPv6-Prefix/Prefix-length:	2009:db9:2229:f1::

Figure 4-8 IPv6 General Prefix Configuration

CLI – This example creates a general network prefix of 2009:DB9:2229::/48.

```
Console(config)#ipv6 general-prefix rd 2009:DB9:2229::/48           41-8
Console(config)#end
Console#show ipv6 general-prefix                                    41-9
IPv6 general prefix: rd
2009:DB9:2229::/48
Console#
```

Configuring Neighbor Detection Protocol and Static Entries

IPv6 Neighbor Discovery Protocol supersedes IPv4 Address Resolution Protocol in IPv6 networks. IPv6 nodes on the same network segment use Neighbor Discovery to discover each other's presence, to determine each other's link-layer addresses, to find routers and to maintain reachability information about the paths to active neighbors. The key parameters used to facilitate this process are the number of attempts made to verify whether or not a duplicate address exists on the same network segment, and the interval between neighbor solicitations used to verify reachability information.

Command Attributes

Protocol Settings

- **VLAN** – VLAN ID (Range: 1-4093)
- **IPv6 ND DAD Attempts** – The number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. (Range: 0-600, Default: 1)
  - Configuring a value of 0 disables duplicate address detection.
  - Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
  - Duplicate address detection is stopped on any interface that has been suspended (see “Creating VLANs” on page 11-6). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
  - An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
  - If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
  - If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.
- **IPv6 ND NS Interval** – The interval between transmitting IPv6 neighbor solicitation messages on an interface. (Range: 1000-3600000 milliseconds;
  Default: 1000 milliseconds is used for neighbor discovery operations,
  0 milliseconds is advertised in router advertisements)
  - This attribute specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

  - When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.

Current Neighbor Cache Table

- **IPv6 Address** – IPv6 address of neighbor device.
- **Age** – The time since the address was verified as reachable (in minutes). A static entry is indicated by the value “Permanent.”
- **Link-layer Address** – Physical layer MAC address.
- **State** – The current state for an entry.

  The following states are used for dynamic entries:

  - INCMP (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message.
  - REACH (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets.
  - STALE - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent.
  - DELAY - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the switch will send a neighbor solicitation message and change the state to PROBE.
  - PROBE - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received.
  - ???? - Unknown state.

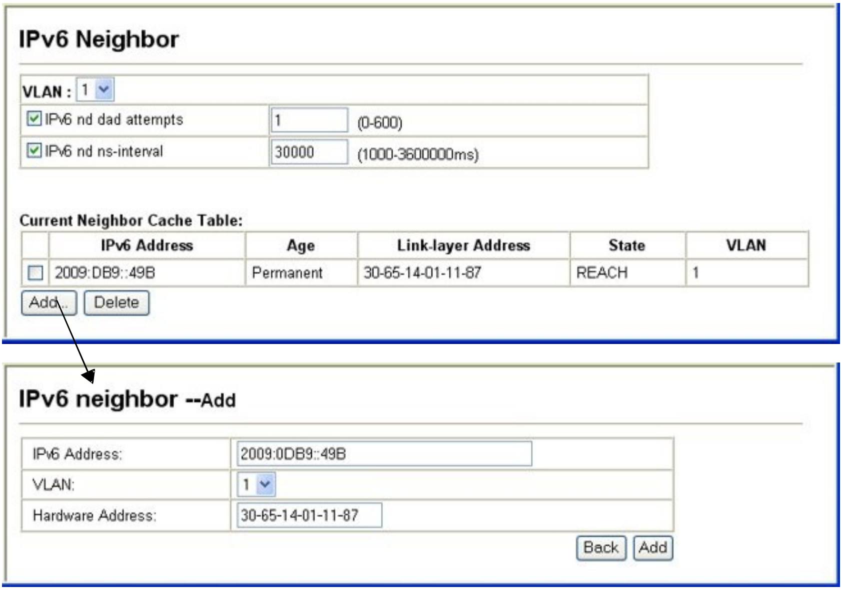
  The following states are used for static entries:

  - INCMP (Incomplete) -The interface for this entry is down.
  - REACH (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
- **VLAN** – VLAN interface from which the address was reached.

Adding Static Neighbors (IPv6 Neighbor -- Add)

- **IPv6 Address** – The IPv6 address of a neighbor device that can be reached through one of the network interfaces configured on this switch. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- **VLAN** – VLAN ID (Range: 1-4093)
- **Hardware Address** – The 48-bit MAC layer address for the neighbor device. This address must be formatted as six hexadecimal pairs separated by hyphens.

Web – Click System, IPv6 Configuration, IPv6 ND Neighbor. To configure the Neighbor Detection protocol settings, select a VLAN interface, set the number of attempts allowed for duplicate address detection, set the interval for neighbor solicitation messages, and click Apply. To configure static neighbor entries, click Add, fill in the IPv6 address, VLAN interface and hardware address. Then click Add.



IPv6 Neighbor

VLAN : 1

☑ IPv6 nd dad attempts	1	(0-600)
☑ IPv6 nd ns-interval	30000	(1000-3600000ms)

Current Neighbor Cache Table:

	IPv6 Address	Age	Link-layer Address	State	VLAN
□	2009:DB9::49B	Permanent	30-65-14-01-11-87	REACH	1

IPv6 neighbor --Add

IPv6 Address:	2009:0DB9::49B
VLAN:	1
Hardware Address:	30-65-14-01-11-87

Figure 4-9 IPv6 Neighbor Detection and Neighbor Cache

CLI – This example maps a static entry for a global unicast address to a MAC address.

```
Console(config)#interface vlan 1                                     27-1
Console(config-if)#ipv6 nd dad attempts 5                           41-27
Console(config-if)#ipv6 nd ns-interval 30000                        41-29
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::1034:11FF:FE11:4321/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64    [
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF11:4321/104
MTU is 1280 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 30000 milliseconds
Console#configure
Console(config)#ipv6 neighbor 2009:0DB9::49A vlan 1
   30-65-14-01-11-87                                                41-26
Console(config)#end
Console#show ipv6 neighbors                                         41-30
IPv6 Address              Age         Link-layer Addr    State       Vlan
2009:DB9:2229::77         Permanent  30-65-14-01-11-87  REACH       1
Console#
```

Configuring Support for Jumbo Frames

The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

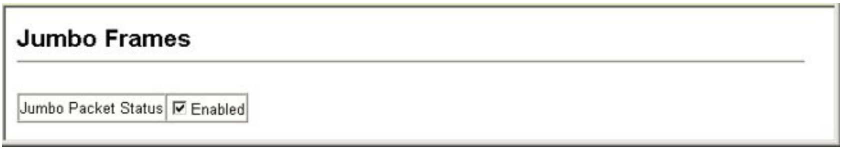
Command Usage

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Command Attributes

Jumbo Packet Status – Configures support for jumbo frames. (Default: Disabled)

Web – Click System, Jumbo Frames. Enable or disable support for jumbo frames, and click Apply.



Jumbo Frames

Jumbo Packet Status ☑ Enabled

Figure 4-10 Configuring Support for Jumbo Frames

CLI – This example enables jumbo frames globally for the switch.

```
Console(config)#jumbo frame                                          23-9
Console(config)#
```

Managing Firmware

You can upload/download firmware to or from a TFTP server, or copy files to and from switch units in a stack. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. You can also set the switch to use new firmware without overwriting the previous version. You must specify the method of file transfer, along with the file type and file names as required.

Command Attributes

- File Transfer Method – The firmware copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
  - file to unit – Copies a file from this switch to another unit in the stack.
  - unit to file – Copies a file from another unit in the stack to this switch.

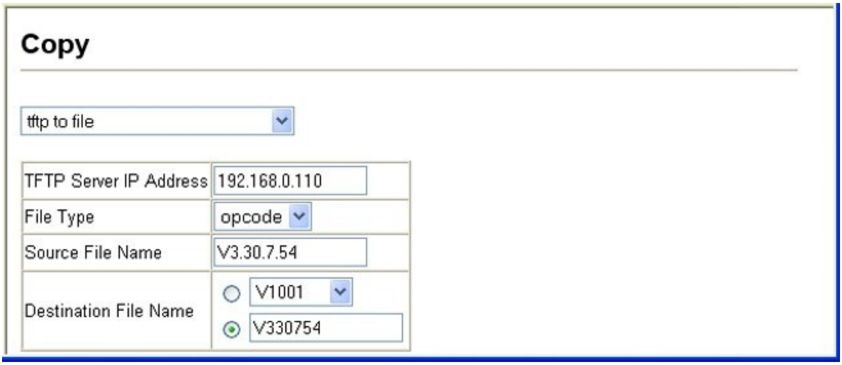
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify opcode (operational code) to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- **Source/Destination Unit** – Stack unit. (Range: 1 - 8)

Note: Up to two copies of the system software (i.e., the runtime firmware) can be stored in the file directory on the switch. The currently designated startup version of this file cannot be deleted.

Downloading System Software from a Server

When downloading runtime code, you can specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, File Management, Copy Operation. Select "tftp to file" as the file transfer method, enter the IP address of the TFTP server, set the file type to "opcode," enter the file name of the software to download, select a file on the switch to overwrite or specify a new file name, then click Apply. If you replaced the current firmware used for startup and want to start using the new operation code, reboot the system via the System/Reset menu.



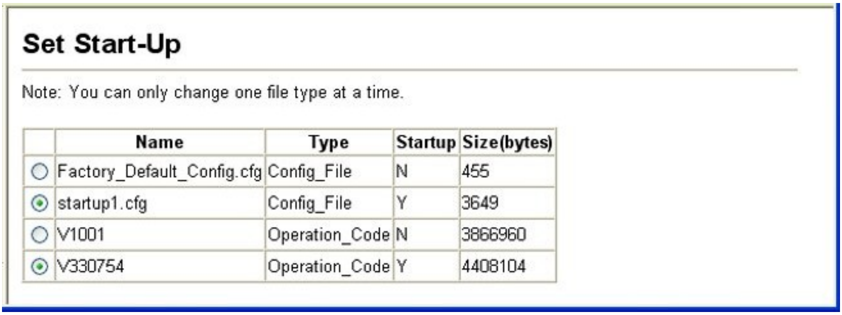
Copy

tftp to file

TFTP Server IP Address	192.168.0.110
File Type	opcode
Source File Name	V3.30.7.54
Destination File Name	○ V1001 ● V330754

Figure 4-11 Copy Firmware

If you download to a new destination file, go to the File Management, Set Start-Up menu, mark the operation code file used at startup, and click Apply. To start the new firmware, reboot the system via the System/Reset menu.



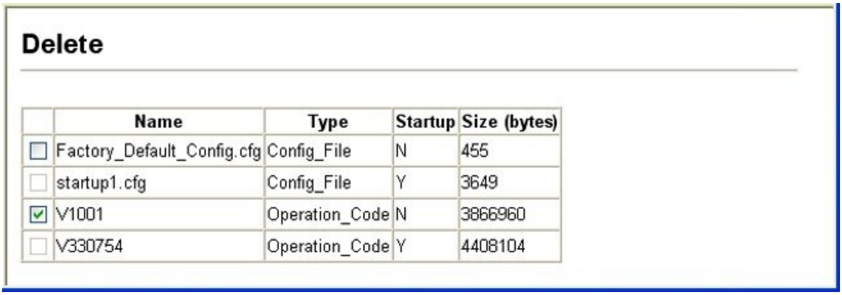
Set Start-Up

Note: You can only change one file type at a time.

	Name	Type	Startup	Size(bytes)
○	Factory_Default_Config.cfg	Config_File	N	455
●	startup1.cfg	Config_File	Y	3649
○	V1001	Operation_Code	N	3866960
●	V330754	Operation_Code	Y	4408104

Figure 4-12 Setting the Startup Code

To delete a file select System, File Management, Delete. Select the file name from the given list by checking the tick box and click Apply. Note that the file currently designated as the startup code cannot be deleted.



Delete

	Name	Type	Startup	Size (bytes)
□	Factory_Default_Config.cfg	Config_File	N	455
□	startup1.cfg	Config_File	Y	3649
☑	V1001	Operation_Code	N	3866960
□	V330754	Operation_Code	Y	4408104

Figure 4-13 Deleting Files

CLI – To download new firmware form a TFTP server, enter the IP address of the TFTP server, select “config” as the file type, then enter the source and destination file names. When the file has finished downloading, set the new file to start up the system, and then restart the switch.

To start the new firmware, enter the “reload” command or reboot the system.

```
Console#copy tftp file                                                 23-11
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: V3.1.16.20.bix
Destination file name: V311620
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:V311620                             23-16
Console(config)#exit
Console#reload                                                          22-4
```

Saving or Restoring Configuration Settings

You can upload/download configuration settings to/from a TFTP server, or copy files to and from switch units in a stack. The configuration file can be later downloaded to restore the switch’s settings.

Command Attributes

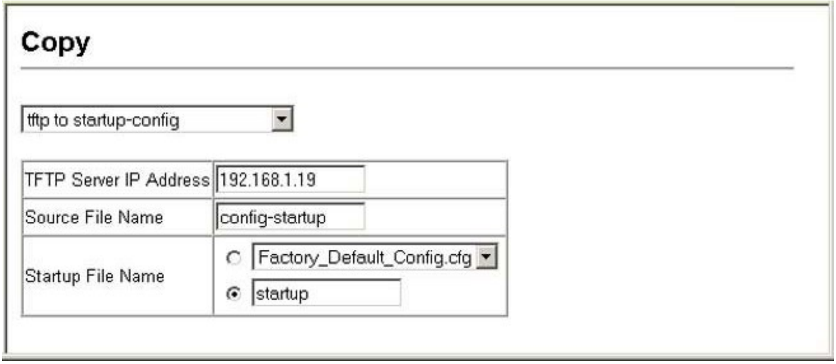
- File Transfer Method – The configuration copy operation includes these options:
  - file to file – Copies a file within the switch directory, assigning it a new name.
  - file to running-config – Copies a file in the switch to the running configuration.
  - file to startup-config – Copies a file in the switch to the startup configuration.
  - file to tftp – Copies a file from the switch to a TFTP server.
  - running-config to file – Copies the running configuration to a file.
  - running-config to startup-config – Copies the running config to the startup config.
  - running-config to tftp – Copies the running configuration to a TFTP server.
  - startup-config to file – Copies the startup configuration to a file on the switch.
  - startup-config to running-config – Copies the startup config to the running config.
  - startup-config to tftp – Copies the startup configuration to a TFTP server.
  - tftp to file – Copies a file from a TFTP server to the switch.
  - tftp to running-config – Copies a file from a TFTP server to the running config.
  - tftp to startup-config – Copies a file from a TFTP server to the startup config.
  - file to unit – Copies a file from this switch to another unit in the stack.
  - unit to file – Copies a file from another unit in the stack to this switch.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify config (configuration) to copy configuration settings.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)
- **Source/Destination Unit** – Stack unit. (Range: 1 - 8)

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

Downloading Configuration Settings from a Server

You can download the configuration file under a new file name and then set it as the startup file, or you can specify the current startup configuration file as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the switch.

Web – Click System, File Management, Copy Operation. Choose “tftp to startup-config” or “tftp to file,” and enter the IP address of the TFTP server. Specify the name of the file to download, select a file on the switch to overwrite or specify a new file name, and then click Apply.

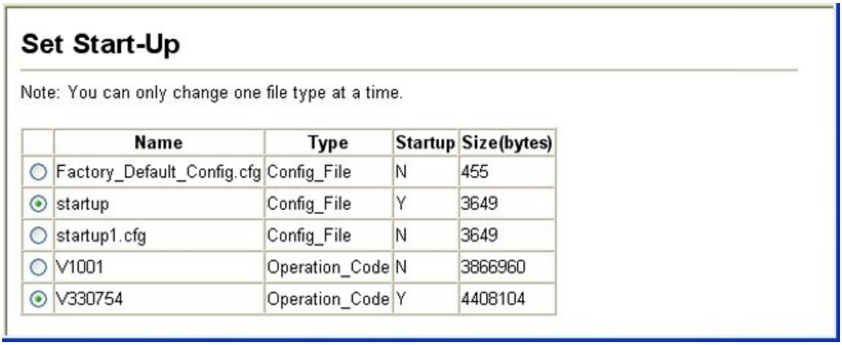


tftp to startup-config

TFTP Server IP Address	192.168.1.19
Source File Name	config-startup
Startup File Name	○ Factory_Default_Config.cfg ● startup

Figure 4-14 Downloading Configuration Settings for Start-Up

If you download to a new file name using “tftp to startup-config” or “tftp to file,” the file is automatically set as the start-up configuration file. To use the new settings, reboot the system via the System/Reset menu. You can also select any configuration file as the start-up configuration by using the System/File Management/Set Start-Up page.



Note: You can only change one file type at a time.

	Name	Type	Startup	Size(bytes)
○	Factory_Default_Config.cfg	Config_File	N	455
●	startup	Config_File	Y	3649
○	startup1.cfg	Config_File	N	3649
○	V1001	Operation_Code	N	3866960
●	V330754	Operation_Code	Y	4408104

Figure 4-15 Setting the Startup Configuration Settings

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the switch, and then restart the switch.

```
Console#copy tftp startup-config                                        23-11
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload
```

To select another configuration file as the start-up configuration, use the **boot system** command and then restart the switch.

```
Console#config
Console(config)#boot system config: startup                             23-16
Console(config)#exit
Console#reload                                                           22-4
```

Console Port Settings

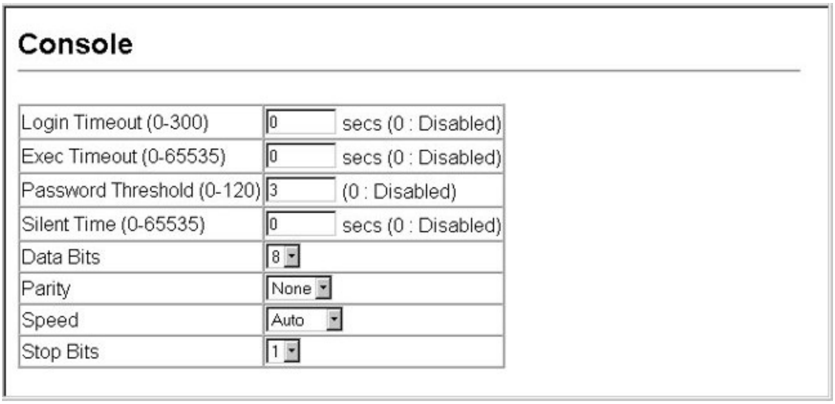
You can access the onboard configuration program by attaching a VT100 compatible device to the switch’s serial console port. Management access through the console port is controlled by various parameters, including a password, timeouts, and basic communication settings. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 0)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 0 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535; Default: 0)
- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)

- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud, Auto; Default: Auto)
- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)
- **Password**[1] – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login**[1] – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Console. Specify the console port connection parameters as required, then click Apply.



Console

Login Timeout (0-300)	0 secs (0 : Disabled)
Exec Timeout (0-65535)	0 secs (0 : Disabled)
Password Threshold (0-120)	3 (0 : Disabled)
Silent Time (0-65535)	0 secs (0 : Disabled)
Data Bits	8
Parity	None
Speed	Auto
Stop Bits	1

Figure 4-16 Configuring the Console Port

[1] CLI only.

CLI – Enter Line Configuration mode for the console, then specify the connection parameters as required. To display the current console port settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line console                                        23-17
Console(config-line)#login local                                    23-18
Console(config-line)#password 0 secret                              23-19
Console(config-line)#timeout login response 0                       23-20
Console(config-line)#exec-timeout 0                                 23-20
Console(config-line)#password-thresh 5                              23-21
Console(config-line)#silent-time 60                                 23-22
Console(config-line)#databits 8                                     23-22
Console(config-line)#parity none                                    23-23
Console(config-line)#speed auto                                     23-23
Console(config-line)#stopbits 1                                     23-24
Console(config-line)#end
Console#show line console                                           23-25
 Console configuration:
  Password threshold:  5 times
  Interactive timeout: Disabled
  Login timeout:        Disabled
  Silent time:         60
  Baudrate:             auto
  Databits:            8
  Parity:               none
  Stopbits:            1
Console#
```

Telnet Settings

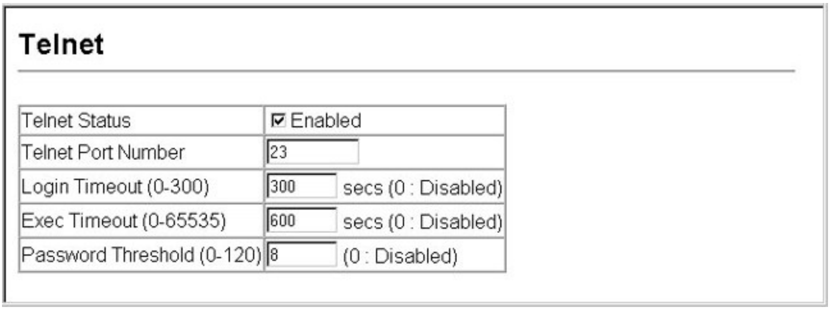
You can access the onboard configuration program over the network using Telnet (i.e., a virtual terminal). Management access via Telnet can be enabled/disabled and other various parameters set, including the TCP port number, timeouts, and a password. These parameters can be configured via the web or CLI interface.

Command Attributes

- **Telnet Status** – Enables or disables Telnet access to the switch. (Default: Enabled)
- **Telnet Port Number** – Sets the TCP port number for Telnet on the switch. (Default: 23)
- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 300 seconds)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)

- **Password**[2] – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. (Default: No password)
- **Login**[2] – Enables password checking at login. You can select authentication by a single global password as configured for the Password parameter, or by passwords set up for specific user-name accounts. (Default: Local)

Web – Click System, Line, Telnet. Specify the connection parameters for Telnet access, then click Apply.



Telnet

Telnet Status	☑ Enabled
Telnet Port Number	23
Login Timeout (0-300)	300 secs (0 : Disabled)
Exec Timeout (0-65535)	600 secs (0 : Disabled)
Password Threshold (0-120)	8 (0 : Disabled)

Figure 4-17 Configuring the Telnet Interface

CLI – Enter Line Configuration mode for a virtual terminal, then specify the connection parameters as required. To display the current virtual terminal settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line vty                                           23-17
Console(config-line)#login local                                   23-18
Console(config-line)#password 0 secret                             23-19
Console(config-line)#timeout login response 300                    23-20
Console(config-line)#exec-timeout 600                              23-20
Console(config-line)#password-thresh 3                             23-21
Console(config-line)#end
Console#show line vty                                              23-25
 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout:        300 sec
Console#
```

[2] CLI only.

Configuring Event Logging

The switch allows you to control the logging of error messages, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

System Log Configuration

The system allows you to enable or disable event logging, and specify which levels are logged to RAM or flash memory.

Severe error messages that are logged to flash memory are permanently stored in the switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows you to configure and limit system messages that are logged to flash or RAM memory. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the switch’s permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 4-1 Logging Levels

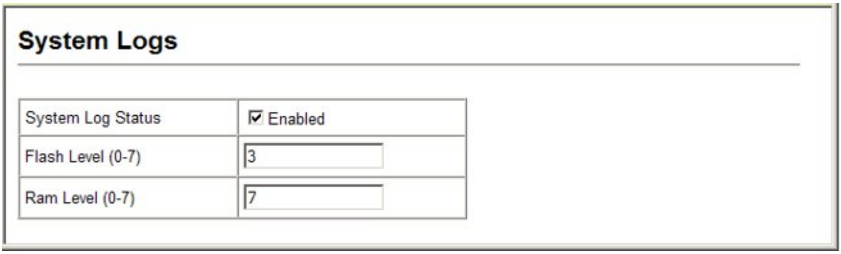
Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (e.g., return false, unexpected return)
3	Error	Error conditions (e.g., invalid input, default used)
2	Critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the switch’s temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, Logs, System Logs. Specify System Log Status, set the level of event messages to be logged to RAM and flash memory, then click Apply.



System Logs

System Log Status	☑ Enabled
Flash Level (0-7)	3
Ram Level (0-7)	7

Figure 4-18 System Logs

CLI – Enable system logging and then specify the level of messages to be logged to RAM and flash memory. Use the **show logging** command to display the current settings.

```
Console(config)#logging on                                        23-26
Console(config)#logging history ram 0                             23-27
Console(config)#
Console#show logging ram                                          23-30
Syslog logging:            Disabled
History logging in RAM: level emergencies
Console#
```

Remote Log Configuration

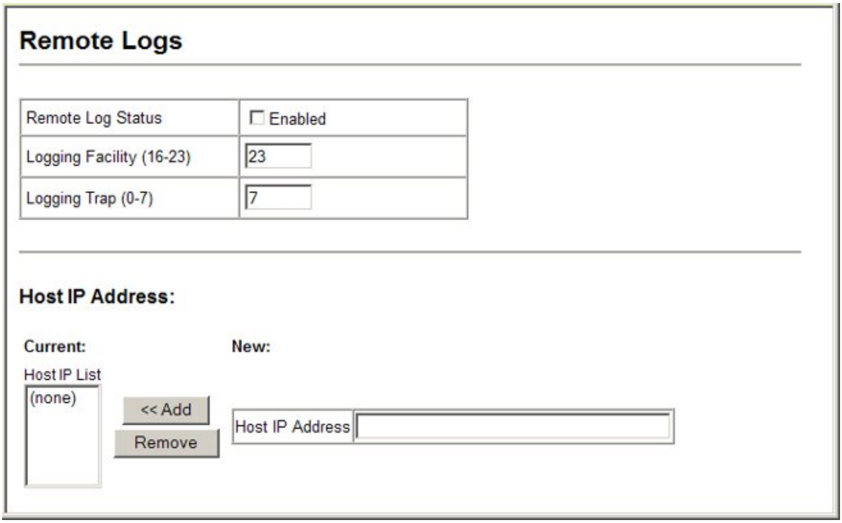
The Remote Logs page allows you to configure the logging of messages that are sent to syslog servers or other management stations. You can also limit the event messages sent to only those messages at or above a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

  The attribute specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Host IP List** – Displays the list of remote server IP addresses that will receive syslog messages. The maximum number of host IP addresses allowed is five.
- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

Web – Click System, Logs, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add. To delete an IP address, click the entry in the Host IP List, and then click Remove.



Remote Logs

Remote Log Status	□ Enabled
Logging Facility (16-23)	23
Logging Trap (0-7)	7

Host IP Address:

Current:

Host IP List

(none)

New:

Host IP Address

Figure 4-19 Remote Logs

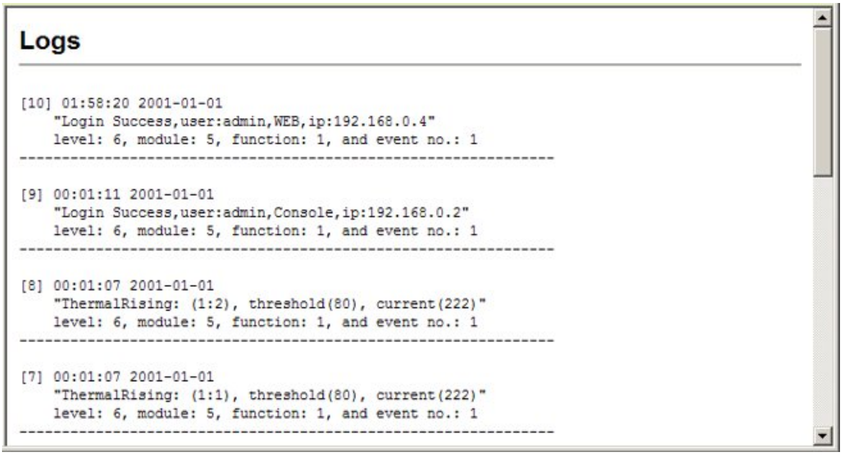
CLI – Enter the syslog server host IP address, choose the facility type and set the logging trap.

```
Console(config)#logging host 10.1.0.9                                    23-28
Console(config)#logging facility 23                                      23-28
Console(config)#logging trap 4                                           23-29
Console(config)#logging trap
Console(config)#exit
Console#show logging trap                                                23-30
Syslog logging:                 Enabled
REMOTELOG status:               Disabled
REMOTELOG facility type:        local use 7
REMOTELOG level type:           Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#
```

Displaying Log Messages

Use the Logs page to scroll through the logged system and event messages. The switch can store up to 2048 log entries in temporary random access memory (RAM; i.e., memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Log, Logs.



Logs

```
[10] 01:58:20 2001-01-01
    "Login Success,user:admin,WEB,ip:192.168.0.4"
    level: 6, module: 5, function: 1, and event no.: 1
----------------------------------------------------------------

[9] 00:01:11 2001-01-01
    "Login Success,user:admin,Console,ip:192.168.0.2"
    level: 6, module: 5, function: 1, and event no.: 1
----------------------------------------------------------------

[8] 00:01:07 2001-01-01
    "ThermalRising: (1:2), threshold(80), current(222)"
    level: 6, module: 5, function: 1, and event no.: 1
----------------------------------------------------------------

[7] 00:01:07 2001-01-01
    "ThermalRising: (1:1), threshold(80), current(222)"
    level: 6, module: 5, function: 1, and event no.: 1
----------------------------------------------------------------
```

Figure 4-20 Displaying Logs

CLI – This example shows the event message stored in RAM.

```
Console#show log ram                                                 23-30
[10]01/01/2001 01:58:20 snmp:"Login Success,user:admin,WEB,ip:192.168.0.4"
[9]01/01/2001 00:01:11 snmp:"Login Success,user:admin,Console,ip:192.168.0.2"
[8]01/01/2001 00:01:07 snmp:"ThermalRising: (1:2), threshold(80), current(222)"
[7]01/01/2001 00:01:07 snmp:"ThermalRising: (1:1), threshold(80), current(222)"
:
```

Sending Simple Mail Transfer Protocol Alerts

To alert system administrators of problems, the switch can use SMTP (Simple Mail Transfer Protocol) to send email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

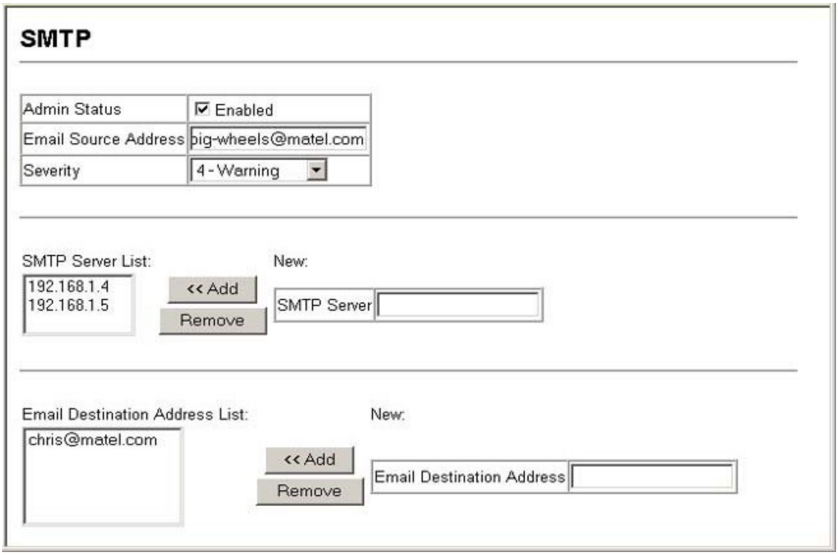
Command Attributes

- **Admin Status** – Enables/disables the SMTP function. (Default: Enabled)
- **Email Source Address** – Sets the email address used for the “From” field in alert messages. You may use a symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.
- **Severity** – Sets the syslog severity threshold level (see table on page 4-30) used to trigger alert messages. All events at this level or higher will be sent to the

configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)

- **SMTP Server List** – Specifies a list of up to three recipient SMTP servers. The switch attempts to connect to the other listed servers if the first fails. Use the New SMTP Server text field and the Add/Remove buttons to configure the list.
- **Email Destination Address List** – Specifies the email recipients of alert messages. You can specify up to five recipients. Use the New Email Destination Address text field and the Add/Remove buttons to configure the list.

Web – Click System, Log, SMTP. Enable SMTP, specify a source email address, and select the minimum severity level. To add an IP address to the SMTP Server List, type the new IP address in the SMTP Server field and click Add. To delete an IP address, click the entry in the SMTP Server List and click Remove. Specify up to five email addresses to receive the alert messages, and click Apply.



SMTP

Admin Status	☑ Enabled
Email Source Address	big-wheels@matel.com
Severity	4 - Warning

SMTP Server List:
192.168.1.4
192.168.1.5

New: SMTP Server

Email Destination Address List:
chris@matel.com

New: Email Destination Address

Figure 4-21 Enabling and Configuring SMTP Alerts

CLI – Enter the IP address of at least one SMTP server, set the syslog severity level to trigger an email message, and specify the switch (source) and up to five recipient (destination) email addresses. Enable SMTP with the **logging sendmail** command to complete the configuration. Use the **show logging sendmail** command to display the current SMTP configuration.

```
Console(config)#logging sendmail host 192.168.1.4                  23-32
Console(config)#logging sendmail level 3                           23-33
Console(config)#logging sendmail source-email
   big-wheels@matel.com                                            23-33
Console(config)#logging sendmail destination-email
   chris@matel.com                                                 23-34
Console(config)#logging sendmail                                   23-34
Console(config)#exit
Console#show logging sendmail                                      23-35
SMTP servers
-----------------------------------------------
  1. 192.168.1.4

SMTP minimum severity level: 4

SMTP destination email addresses
-----------------------------------------------
  1. chris@matel.com

SMTP source email address: big-wheels@matel.com

SMTP status:                Enabled
Console#
```

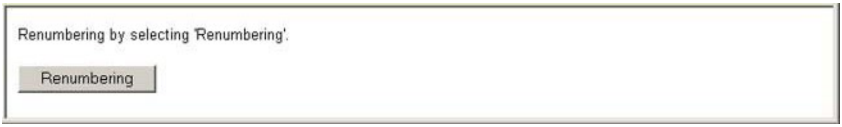
Renumbering the Stack

If the units are no longer numbered sequentially after several topology changes or failures, you can reset the unit numbers using the “Renumbering” command. Just remember to save the new configuration settings to a startup configuration file prior to powering off the stack Master.

Command Usage

- The startup configuration file maps configuration settings to each switch in the stack based on the unit identification number. You should therefore remember to save the current configuration after renumbering the stack.
- For a line topology, the stack is numbered from top to bottom, with the first unit in the stack designated at unit 1. For a ring topology, the Master unit taken as the top of the stack and is numbered as unit 1, and all other units are numbered sequentially down through the ring.

Web – Click System, Renumbering.



Renumbering by selecting 'Renumbering'.

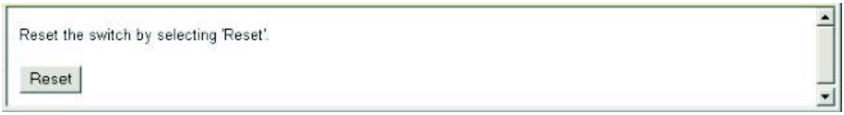
Figure 4-22 Renumbering the Stack

CLI – This example renumbers all units in the stack.

```
Console#switch all renumber                                         23-2
Console#
```

Resetting the System

Web – Click System, Reset. Click the Reset button to restart the switch. When prompted, confirm that you want reset the switch.



Reset the switch by selecting 'Reset'.

Figure 4-23 Resetting the System

CLI – Use the reload command to restart the switch.

```
Console#reload                                                       22-4
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

Setting the System Clock

Simple Network Time Protocol (SNTP) allows the switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. You can also manually set the clock using the Current Time page as described in the next section. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the switch periodically sends a request for a time update to a configured time server. You can configure up to three time server IP addresses. The switch will attempt to poll each server in the configured sequence.

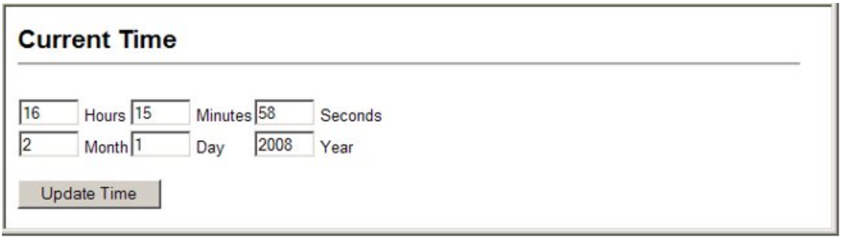
Setting the Current Time

You can manually set the system clock if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Command Attributes

- **Hours** – Hour in 24-hour format. (Range: 0 - 23)
- **Minutes** – Minute. (Range: 0 - 59)
- **Seconds** – Second. (Range: 0 - 59)
- **Month** – Month. (Range: 1 - 12)
- **Day** – Day of month. (Range: 1 - 31)
- **Year** – Year (4-digit). (Range: 2001 - 2100)
- **Update Time** – Click this button to display the time now in use by the system clock.

Web – Select SNTP, Current Time. Set the date and time, and click Apply.



Current Time

16 Hours 15 Minutes 58 Seconds
2 Month 1 Day 2008 Year

Figure 4-24 Current Time

CLI – This example sets the system clock to 16:15:58, February 1st, 2008.

```
Console#calendar set 16 15 58 february 1 2008
Console#
```

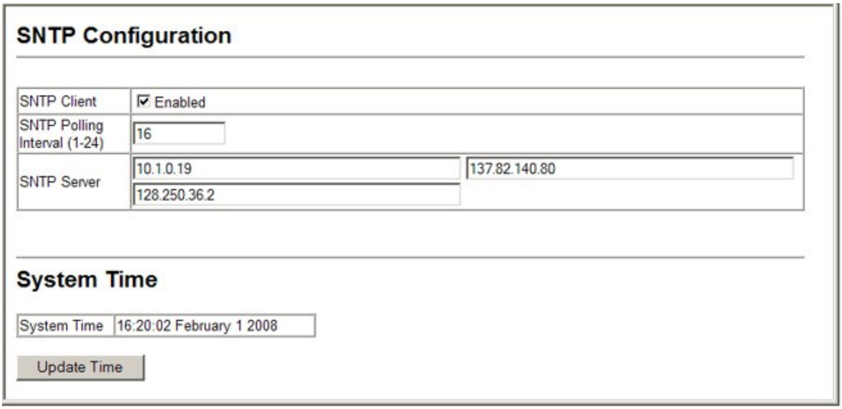
Configuring SNTP

You can configure the switch to send time synchronization requests to time servers.

Command Attributes

- **SNTP Client** – Configures the switch to operate as an SNTP client. This requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16384 seconds; Default: 16 seconds)
- **SNTP Server** – Sets the IP address for up to three time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.
- **Update Time** – Click the Update Time button to send a request to the configured SNTP servers to immediately update the system time.

Web – Select SNTP, Configuration. Modify any of the required SNTP parameters, and click Apply. To send an immediate request to the configured servers, click Update Time.



SNTP Client	☑ Enabled
SNTP Polling Interval (1-24)	16
SNTP Server	10.1.0.19 137.82.140.80 128.250.36.2

System Time	16:20:02 February 1 2008

Figure 4-25 SNTP Configuration

CLI – This example configures the switch to operate as an SNTP client and then displays the current time and settings.

```
Console(config)#sntp client                                        23-36
Console(config)#sntp poll 16                                       23-37
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2   23-37
Console(config)#sntp update-time                                   23-38
Console(config)#exit
Console#show sntp                                                  23-38
Current time:   Jan   6 14:56:05 2004
Poll interval: 60
Current   mode:   unicast
SNTP status : Enabled
SNTP server 10.1.0.19 137.82.140.80 128.250.36.2
Current server: 128.250.36.2
Console#
```

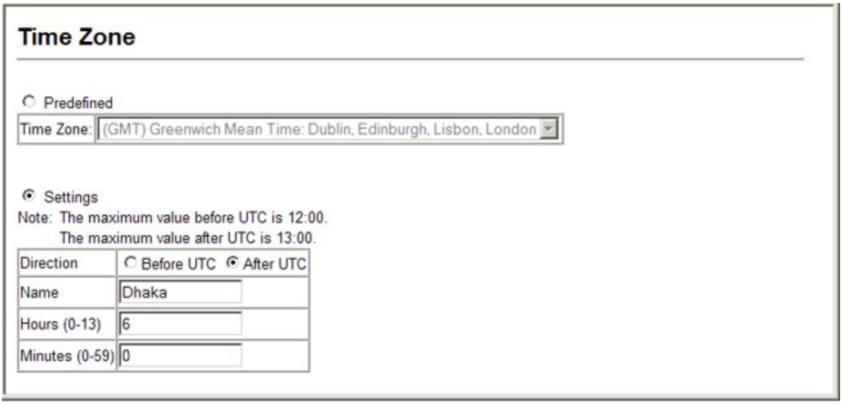
Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth’s prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Command Attributes

- **Predefined** – Configures the time zone using predefined settings.
- **Manual Setting** –
  - **Direction** – Configures the time zone to be before (east) or after (west) UTC.
  - **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
  - **Hours (0-13)** – The number of hours before/after UTC.
  - **Minutes (0-59)** – The number of minutes before/after UTC.

Web – Select SNTP, Clock Time Zone. Select one of the predefined time zones, or manually set the offset for your time zone relative to the UTC, and click Apply.



Time Zone

○ Predefined

Time Zone: (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

● Settings

Note: The maximum value before UTC is 12:00.
The maximum value after UTC is 13:00.

Direction	○ Before UTC ● After UTC
Name	Dhaka
Hours (0-13)	6
Minutes (0-59)	0

Figure 4-26 Clock Time Zone

CLI - This example shows how to select one of the predefined time zones.

```
Console(config)#clock timezone-predefined GMT-0930-Taiohae          23-39
Console#
```

This example shows how to manually set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC     23-39
Console#
```

Configuring Summer Time

Use the Summer Time page to set the system clock forward during the summer months (also known as daylight savings time).

Command Usage

In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.

Command Attributes

General Configuration

- **Summer Time in Effect** – Shows if the system time has been adjusted.
- **Status** – Shows if summer time is set to take effect during the specified period.
- **Name** – Name of the time zone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- **Mode** – Selects one of the following configuration modes.

Predefined Mode – Configures the summer time status and settings for the switch using predefined configurations for several major regions of the world. To specify the time corresponding to your local time when summer-time is in effect, select the predefined summer-time time zone appropriate for your location.

Table 4-2 Predefined Summer-Time Parameters

Region	Start Time, Day, Week, & Month	End Time, Day, Week, & Month	Rel. Offset
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 min
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 min
USA	02:00:00, Sunday, Week 2 of March	02:00:00, Sunday, Week 1 of November	60 min

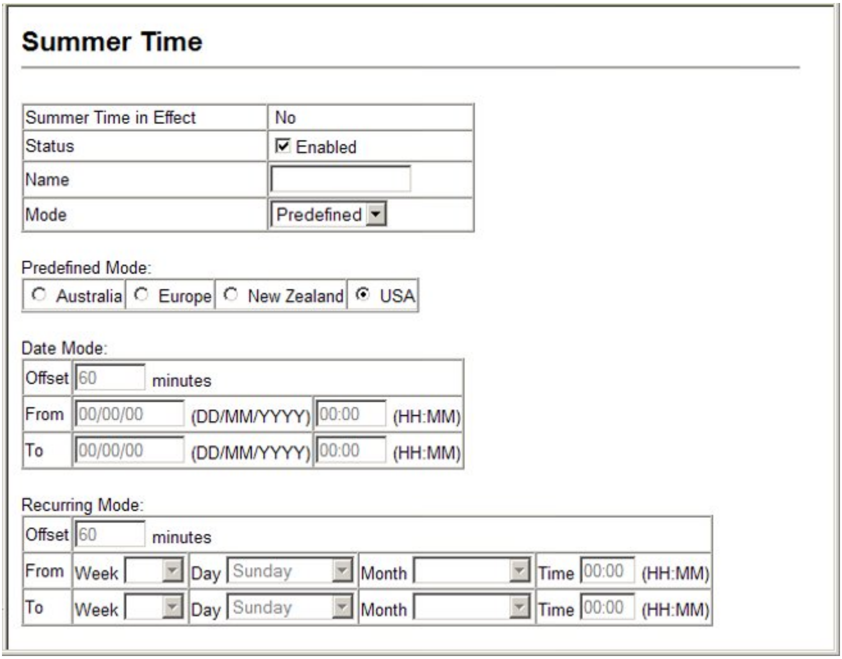
Date Mode – Sets the start, end, and offset times of summer-time for the switch on a one-time basis. This mode sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer-time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

- **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)
- **From** – Start time for summer-time offset.
- **To** – End time for summer-time offset.

Recurring Mode – Sets the start, end, and offset times of summer-time for the switch on a recurring basis. This mode sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer-time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

- **Offset** – Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)
- **From** – Start time for summer-time offset.
- **To** – End time for summer-time offset.

Web – Select SNTP, Summer Time. Select one of the configuration modes, configure the relevant attributes, enable summer time status, and click Apply.



Summer Time

Summer Time in Effect	No
Status	☑ Enabled
Name	
Mode	Predefined ▾

Predefined Mode:

○ Australia	○ Europe	○ New Zealand	● USA

Date Mode:

Offset	60 minutes			
From	00/00/00	(DD/MM/YYYY)	00:00	(HH:MM)
To	00/00/00	(DD/MM/YYYY)	00:00	(HH:MM)

Recurring Mode:

Offset	60 minutes			
From	Week ▾	Day Sunday ▾	Month ▾	Time 00:00 (HH:MM)
To	Week ▾	Day Sunday ▾	Month ▾	Time 00:00 (HH:MM)

Figure 4-27 Summer Time

CLI - This example configures summer time to take effect for a predefined zone.

```
Console(config)#clock summer-time MESZ predefined usa                23-41
Console#
```

Chapter 5: Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

Access to the switch using from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it’s own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to “groups” that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as “views.” The switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. The following table shows the security models and levels available and the system default settings.

Table 5-1 SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v1	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v1	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuthNoPriv	public (read only)	defaultview	none	none	Community string only
v2c	noAuthNoPriv	private (read/write)	defaultview	defaultview	none	Community string only
v2c	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	A user name match only
v3	AuthNoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms
v3	AuthPriv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

Note: The predefined default groups and view can be deleted from the system. You can then define customized groups and views for the SNMP clients that require access.

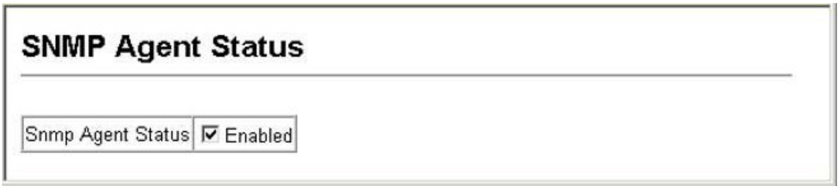
Enabling the SNMP Agent

Enables SNMPv3 service for all management clients (i.e., versions 1, 2c, 3).

Command Attributes

SNMP Agent Status – Enables SNMP on the switch.

Web – Click SNMP, Agent Status. Enable the SNMP Agent by marking the Enabled checkbox, and click Apply.



SNMP Agent Status

Snmp Agent Status ☑ Enabled

Figure 5-1 Enabling the SNMP Agent

CLI – The following example enables SNMP on the switch.

```
Console(config)#snmp-server                                          24-2
Console(config)#
```

Setting Community Access Strings

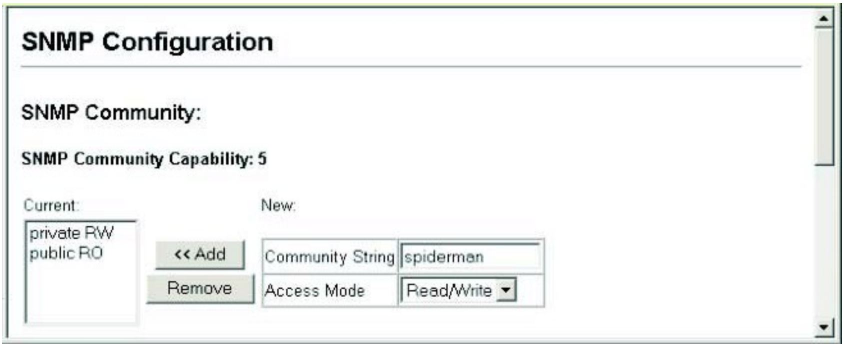
You may configure up to five community strings authorized for management access by clients using SNMP v1 and v2c. All community strings used for IP Trap Managers should be listed in this table. For security reasons, you should consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – The switch supports up to five community strings.
- **Current** – Displays a list of the community strings currently configured.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.

  Default strings: “public” (read-only access), “private” (read/write access)
  Range: 1-32 characters, case sensitive
- **Access Mode** – Specifies the access rights for the community string:
  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.



SNMP Configuration

SNMP Community:

SNMP Community Capability: 5

Current:
private RW
public RO

New:
Community String: spiderman
Access Mode: Read/Write

Figure 5-2 Configuring SNMP Community Strings

CLI – The following example adds the string “spiderman” with read/write access.

```
Console(config)#snmp-server community spiderman rw                     24-3
Console(config)#
```

Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management platforms such as HP OpenView). You can specify up to five management stations that will receive authentication failure messages and other trap messages from the switch.

Command Usage

- If you specify an SNMP Version 3 host, then the “Trap Manager Community String” is interpreted as an SNMP user name. If you use V3 authentication or encryption options (authNoPriv or authPriv), the user name must first be defined in the SNMPv3 Users page (page 5-9). Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the no authentication (noAuth) option, an SNMP user account will be automatically generated, and the switch will authorize SNMP access for the host.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 5-2).
  2. Enable trap informs as described in the following pages.
  3. Create a view with the required notification messages (page 5-17).
  4. Create a group that includes the required notify view (page 5-13).

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 5-2).
  2. Enable trap informs as described in the following pages.
  3. Create a view with the required notification messages (page 5-17).
  4. Create a group that includes the required notify view (page 5-13).
  5. Specify a remote engine ID where the user resides (page 5-8).
  6. Then configure a remote user (page 5-11).

Command Attributes

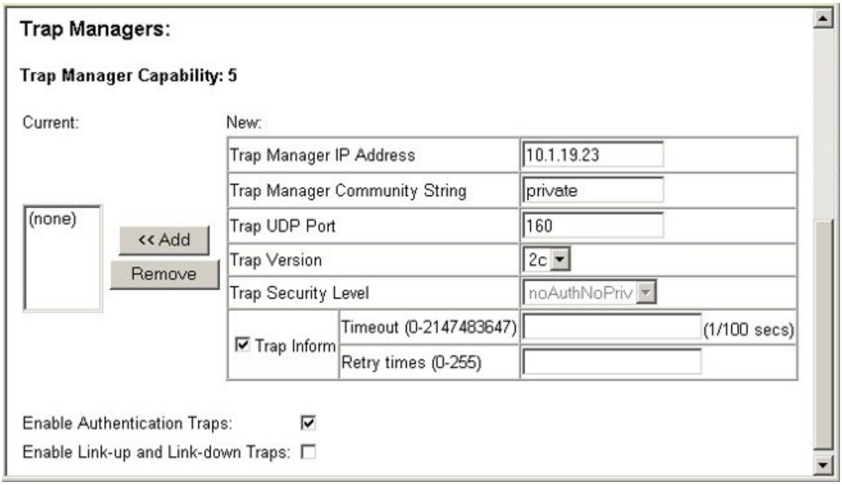
- **Trap Manager Capability** – This switch supports up to five trap managers.
- **Current** – Displays a list of the trap managers currently configured.
- **Trap Manager IP Address** – IP address of a new management station to receive notification messages.
- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. Though you can set this string in the Trap Managers table, we recommend that you define this string in the SNMP Configuration page (for

Version 1 or 2c clients), or define a corresponding “User Name” in the SNMPv3 Users page (for Version 3 clients). (Range: 1-32 characters, case sensitive)

- **Trap UDP Port** – Specifies the UDP port number used by the trap manager.
- **Trap Version** – Indicates if the user is running SNMP v1, v2c, or v3. (Default: v1)
- **Trap Security Level** – When trap version 3 is selected, you must specify one of the following security levels. (Default: noAuthNoPriv)
  - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
  - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Trap Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
  - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Enable Authentication Traps**[3] – Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)
- **Enable Link-up and Link-down Traps**[3] – Issues a notification message whenever a port link is established or broken. (Default: Enabled)

[3] These are legacy notifications and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 5-13).

Web – Click SNMP, Configuration. Enter the IP address and community string for each management station that will receive trap messages, specify the UDP port, SNMP trap version, trap security level (for v3 clients), trap inform settings (for v2c/v3 clients), and then click Add. Select the trap types required using the check boxes for Authentication and Link-up/down traps, and then click Apply.



Trap Managers:

Trap Manager Capability: 5

Current: (none)

New:

Trap Manager IP Address		10.1.19.23
Trap Manager Community String		private
Trap UDP Port		160
Trap Version		2c
Trap Security Level		noAuthNoPriv
☑ Trap Inform	Timeout (0-2147483647)	(1/100 secs)
	Retry times (0-255)	

Enable Authentication Traps: ☑

Enable Link-up and Link-down Traps: □

Figure 5-3 Configuring SNMP Trap Managers

CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 private version 2c
 udp-port 162                                                24-5
Console(config)#snmp-server enable traps authentication      24-7
```

Configuring SNMPv3 Management Access

To configure SNMPv3 management access to the switch, follow these steps:

1. If you want to change the default engine ID, do so before configuring other SNMP parameters.
2. Specify read and write access views for the switch MIB tree.
3. Configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy).
4. Assign SNMP users to groups, along with their specific authentication and privacy passwords.

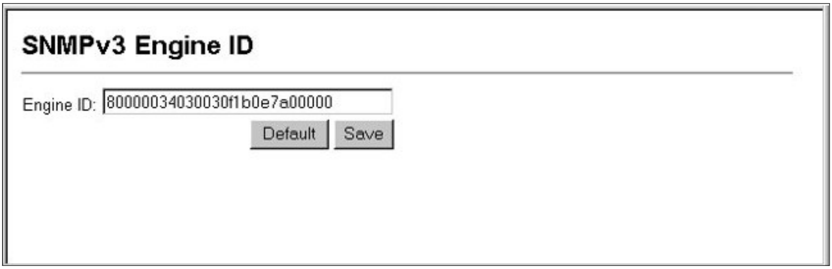
Setting a Local Engine ID

An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engineID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users.

A new engine ID can be specified by entering 9 to 64 hexadecimal characters. If an odd number of characters are specified, a trailing zero is added to the value to fill in the missing octet. For example, the value “123456789” is equivalent to “1234567890”.

Web – Click SNMP, SNMPv3, Engine ID. Enter an ID of up to 64 hexadecimal characters and then click Save.



SNMPv3 Engine ID

Engine ID: 80000034030030f1b0e7a00000

Figure 5-4 Setting the SNMPv3 Engine ID

CLI – This example sets an SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id local 12345abcdef              24-8
Console(config)#exit
Console#show snmp engine-id                                          24-9
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1
Console#
```

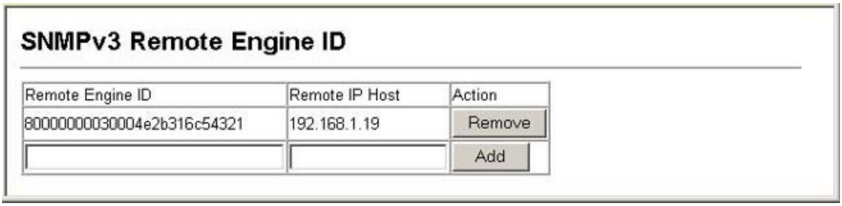
Specifying a Remote Engine ID

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it. (See "Specifying Trap Managers and Trap Types" on page 5-4 and "Configuring Remote SNMPv3 Users" on page 5-11.)

A new engine ID can be specified by entering 9 to 64 hexadecimal characters. If an odd number of characters are specified, a trailing zero is added to the value to fill in the missing octet. For example, the value "123456789" is equivalent to "1234567890".

Web – Click SNMP, SNMPv3, Remote Engine ID. Enter an ID of up to 64 hexadecimal characters and then click Save.



SNMPv3 Remote Engine ID

Remote Engine ID	Remote IP Host	Action
80000000030004e2b316c54321	192.168.1.19	Remove
		Add

Figure 5-5 Setting an Engine ID

CLI – This example specifies a remote SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id remote 54321 192.168.1.19      24-8
Console(config)#exit
Console#show snmp engine-id                                          24-9
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                              IP address
80000000030004e2b316c54321                                        192.168.1.19
Console#
```

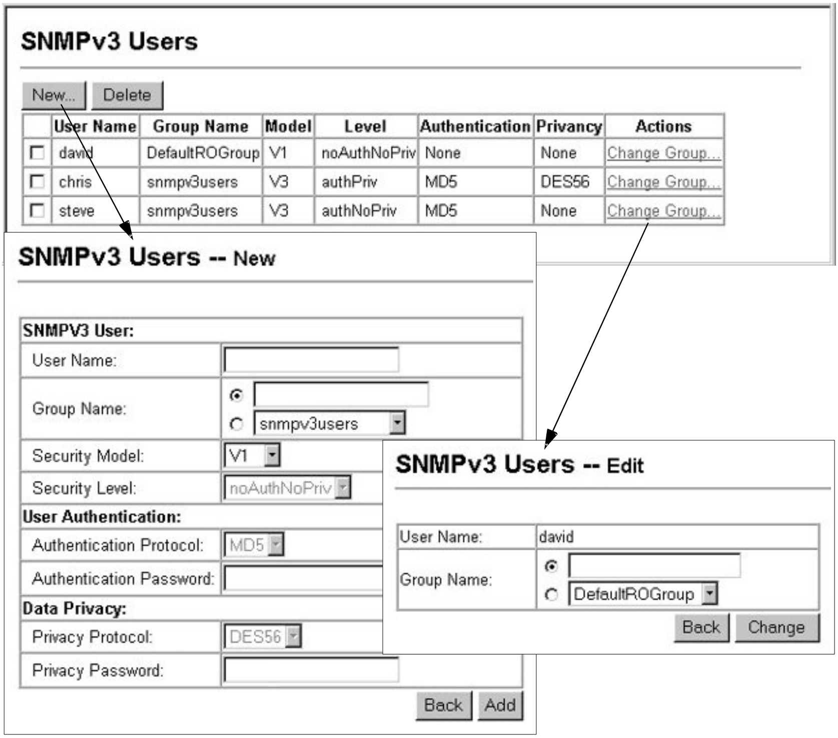
Configuring SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, or notify view.

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.
- **Actions** – Enables the user to be assigned to another SNMPv3 group.

Web – Click SNMP, SNMPv3, Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.



SNMPv3 Users

	User Name	Group Name	Model	Level	Authentication	Privancy	Actions
□	david	DefaultROGroup	V1	noAuthNoPriv	None	None	Change Group...
□	chris	snmpv3users	V3	authPriv	MD5	DES56	Change Group...
□	steve	snmpv3users	V3	authNoPriv	MD5	None	Change Group...

SNMPv3 Users -- New

SNMPV3 User:	
User Name:	
Group Name:	● ○ snmpv3users
Security Model:	V1
Security Level:	noAuthNoPriv
User Authentication:	
Authentication Protocol:	MD5
Authentication Password:	
Data Privacy:	
Privacy Protocol:	DES56
Privacy Password:	

SNMPv3 Users -- Edit

User Name:	david
Group Name:	● ○ DefaultROGroup

Figure 5-6 Configuring SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user chris group r&d v3 auth md5
 greenpeace priv des56 einstien                                  24-14
Console(config)#exit
Console#show snmp user                                           24-15
EngineId: 80000034030001f488f5200000
User Name: chris
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring Remote SNMPv3 Users

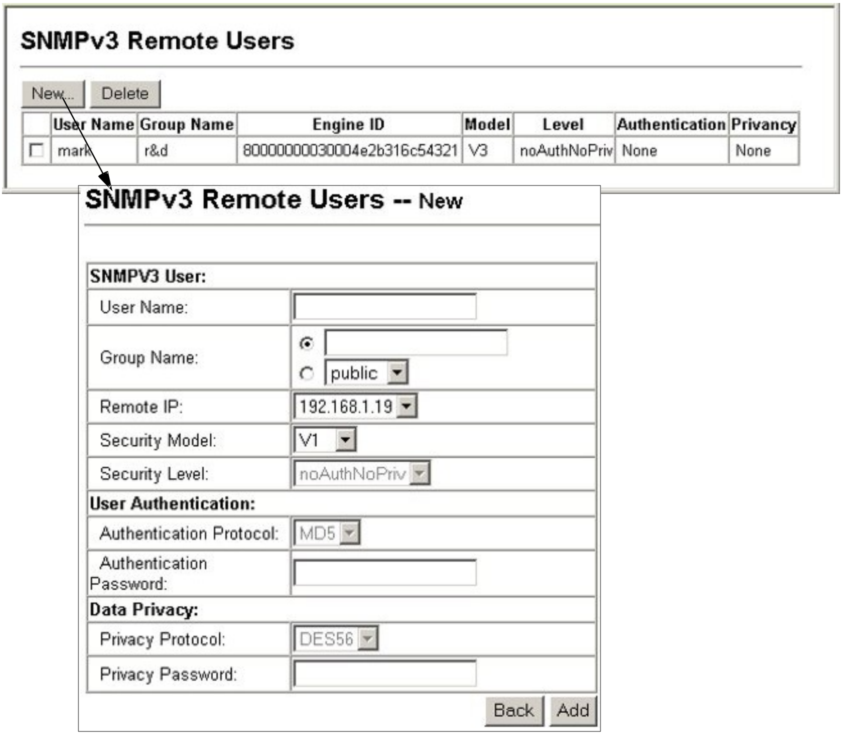
Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read and a write view.

To send inform messages to an SNMPv3 user on a remote device, you must first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. (See “Specifying Trap Managers and Trap Types” on page 5-4 and “Specifying a Remote Engine ID” on page 5-8.)

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Engine ID** – The engine identifier for the SNMP agent on the remote device where the remote user resides. Note that the remote engine identifier must be specified before you configure a remote user. (See “Specifying a Remote Engine ID” on page 5-8.)
- **Remote IP** – The Internet address of the remote device where the user resides.
- **Security Model** – The user security model; SNMP v1, v2c or v3. (Default: v1)
- **Security Level** – The security level used for the user:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication. (Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

Web – Click SNMP, SNMPv3, Remote Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete.



SNMPv3 Remote Users

	User Name	Group Name	Engine ID	Model	Level	Authentication	Privancy
□	mark	r&d	80000000030004e2b316c54321	V3	noAuthNoPriv	None	None

SNMPv3 Remote Users -- New

SNMPV3 User:	
User Name:	
Group Name:	● ○ public
Remote IP:	192.168.1.19
Security Model:	V1
Security Level:	noAuthNoPriv
User Authentication:	
Authentication Protocol:	MD5
Authentication Password:	
Data Privacy:	
Privacy Protocol:	DES56
Privacy Password:	

Figure 5-7 Configuring Remote SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3
 auth md5 greenpeace priv des56 einstien                                  24-14
Console(config)#exit
Console#show  snmp  user                                                  24-15
No user exist.

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonvolatile
Row Status: active

Console#
```

Configuring SNMPv3 Groups

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read, write, and notify views. You can use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

Command Attributes

- **Group Name** – The name of the SNMP group. (Range: 1-32 characters)
- **Model** – The group security model; SNMP v1, v2c or v3.
- **Level** – The security level used for the group:
  - noAuthNoPriv – There is no authentication or encryption used in SNMP communications.
  - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
  - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Read View** – The configured view for read access. (Range: 1-32 characters)
- **Write View** – The configured view for write access. (Range: 1-32 characters)
- **Notify View** – The configured view for notifications. (Range: 1-32 characters)

Table 5-2 Supported Notification Messages

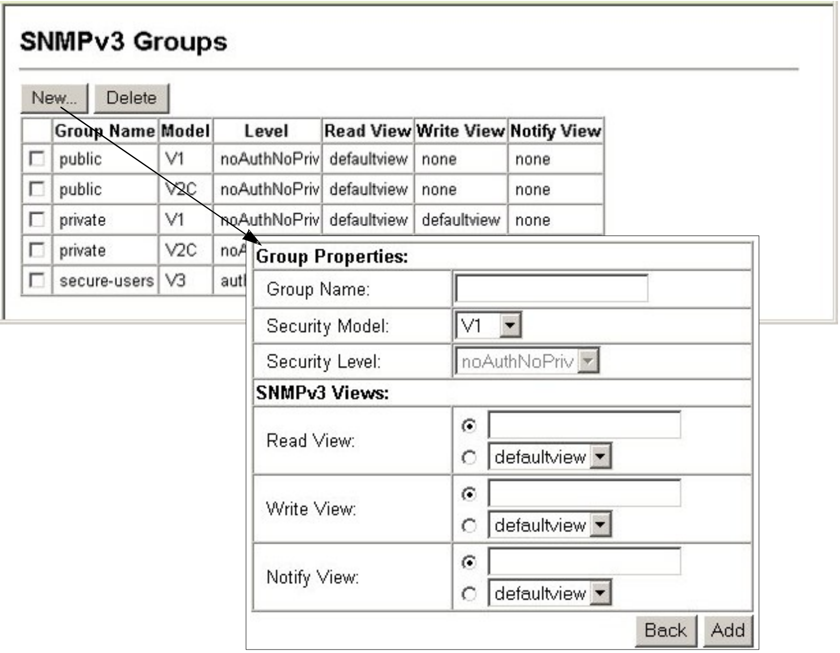
Object Label	Object ID	Description
RFC 1493 Traps		
newRoot	1.3.6.1.2.1.17.0.1	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer immediately subsequent to its election.
topologyChange	1.3.6.1.2.1.17.0.2	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Discarding state. The trap is not sent if a newRoot trap is sent for the same transition.
SNMPv2 Traps		
coldStart	1.3.6.1.6.3.1.1.5.1	A coldStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
warmStart	1.3.6.1.6.3.1.1.5.2	A warmStart trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.
linkDown*	1.3.6.1.6.3.1.1.5.3	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.
linkUp*	1.3.6.1.6.3.1.1.5.4	A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.
authenticationFailure*	1.3.6.1.6.3.1.1.5.5	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.
RMON Events (V2)		
risingAlarm	1.3.6.1.2.1.16.0.1	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.
fallingAlarm	1.3.6.1.2.1.16.0.2	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.

Table 5-2 Supported Notification Messages (Continued)

Object Label	Object ID	Description
Private Traps -		
swPowerStatus ChangeTrap	1.3.6.1.4.1.202.20.57.84.2.1.0.1	This trap is sent when the power state changes.
swFanFailureTrap	1.3.6.1.4.1.202.20.57.84.2.1.0.17	This trap is sent when the fan fails.
swFanRecoverTrap	1.3.6.1.4.1.202.20.57.84.2.1.0.18	This trap is sent when the fan failure has recovered.
swIpFilterRejectTrap	1.3.6.1.4.1.202.20.57.84.2.1.0.40	This trap is sent when an incorrect IP address is rejected by the IP Filter.
swSmtpConnFailure Trap	1.3.6.1.4.1.202.20.57.84.2.1.0.41	This trap is triggered if the SMTP system cannot open a connection to the mail server successfully.
swMainBoardVer MismatchNotificaiton	1.3.6.1.4.1.202.20.57.84.2.1.0.56	This trap is sent when the slave board version is mismatched with the master board version. This trap binds two objects, the first object indicates the master version, whereas the second represents the slave version.
swModuleVer MismatchNotificaiton	1.3.6.1.4.1.202.20.57.84.2.1.0.57	This trap is sent when the slide-in module version is mismatched with the main board version.
swThermalRising Notification	1.3.6.1.4.1.202.20.57.84.2.1.0.58	This trap is sent when the temperature exceeds the switchThermalActionRisingThreshold.
swThermalFalling Notification	1.3.6.1.4.1.202.20.57.84.2.1.0.59	This trap is sent when the temperature falls below the switchThermalActionFallingThreshold.
swModuleInsertion Notificaiton	1.3.6.1.4.1.202.20.57.84.2.1.0.60	This trap is sent when a module is inserted.
swModuleRemoval Notificaiton	1.3.6.1.4.1.202.20.57.84.2.1.0.61	This trap is sent when a module is removed.

* These are legacy notifications and therefore must be enabled in conjunction with the corresponding traps on the SNMP Configuration menu (page 5-6).

Web – Click SNMP, SNMPv3, Groups. Click New to configure a new group. In the New Group page, define a name, assign a security model and level, and then select read, write, and notify views. Click Add to save the new group and return to the Groups list. To delete a group, check the box next to the group name, then click Delete.



SNMPv3 Groups

	Group Name	Model	Level	Read View	Write View	Notify View
□	public	V1	noAuthNoPriv	defaultview	none	none
□	public	V2C	noAuthNoPriv	defaultview	none	none
□	private	V1	noAuthNoPriv	defaultview	defaultview	none
□	private	V2C	noA			
□	secure-users	V3	aut			

Group Properties:

Group Name:	
Security Model:	V1
Security Level:	noAuthNoPriv

SNMPv3 Views:

Read View:	● ○ defaultview
Write View:	● ○ defaultview
Notify View:	● ○ defaultview

Figure 5-8 Configuring SNMPv3 Groups

CLI – Use the **snmp-server group** command to configure a new group, specifying the security model and level, and restricting MIB access to defined read and write views.

```
Console(config)#snmp-server group secure-users v3 priv read defaultview
 write defaultview notify defaultview                                   24-11
Console(config)#exit
Console#show  snmp  group                                               24-12
:
Group Name: secure-users
Security Model: v3
Read View: defaultview
Write View: defaultview
Notify View: defaultview
Storage Type: nonvolatile
Row Status: active

Console#
```

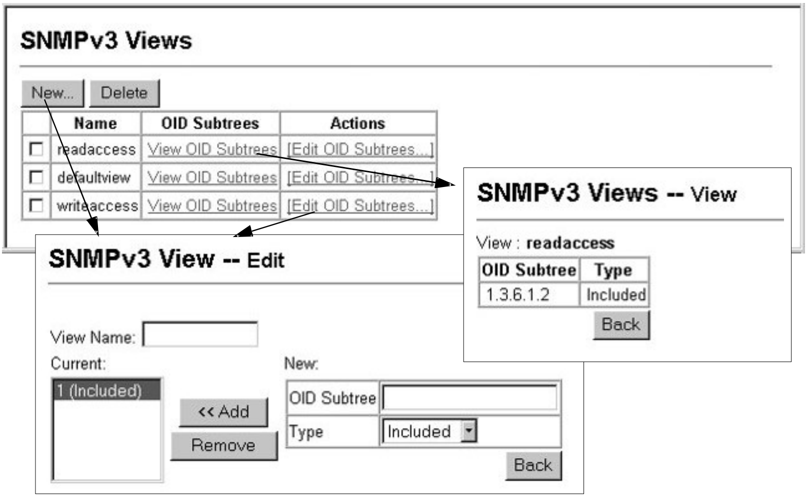
Setting SNMPv3 Views

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The predefined view “defaultview” includes access to the entire MIB tree.

Command Attributes

- **View Name** – The name of the SNMP view. (Range: 1-32 characters)
- **View OID Subtrees** – Shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view.
- **Edit OID Subtrees** – Allows you to configure the object identifiers of branches within the MIB tree. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Web – Click SNMP, SNMPv3, Views. Click New to configure a new view. In the New View page, define a name and specify OID subtrees in the switch MIB to be included or excluded in the view. Click Back to save the new view and return to the SNMPv3 Views list. For a specific view, click on View OID Subtrees to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings. To delete a view, check the box next to the view name, then click Delete.



SNMPv3 Views

	Name	OID Subtrees	Actions
□	readaccess	View OID Subtrees	[Edit OID Subtrees...]
□	defaultview	View OID Subtrees	[Edit OID Subtrees...]
□	writeaccess	View OID Subtrees	[Edit OID Subtrees...]

SNMPv3 Views -- View

View : **readaccess**

OID Subtree	Type
1.3.6.1.2	Included

SNMPv3 View -- Edit

View Name:

Current: 1 (Included)

New:

OID Subtree	
Type	Included

Figure 5-9 Configuring SNMPv3 Views

CLI – Use the **snmp-server view** command to configure a new view. This example view includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
  included                                                           24-10
Console(config)#exit
Console#show snmp view                                               24-11
View Name: ifEntry.a
Subtree OID: 1.3.6.1.2.1.2.2.1.1.*
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: readaccess
Subtree OID: 1.3.6.1.2
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```

Chapter 6: User Authentication

You can restrict management access to this switch and provide secure network access using the following options:

- User Accounts – Manually configure management access rights for users.
- Authentication Settings – Use remote authentication to configure access rights.
- HTTPS Settings – Provide a secure web connection.
- SSH Settings – Provide a secure shell (for secure Telnet access).
- Port Security – Configure secure addresses for individual ports.
- 802.1X – Use IEEE 802.1X port authentication to control access to specific ports.
- IP Filter – Filters management access to the web, SNMP or Telnet interface.

Configuring User Accounts

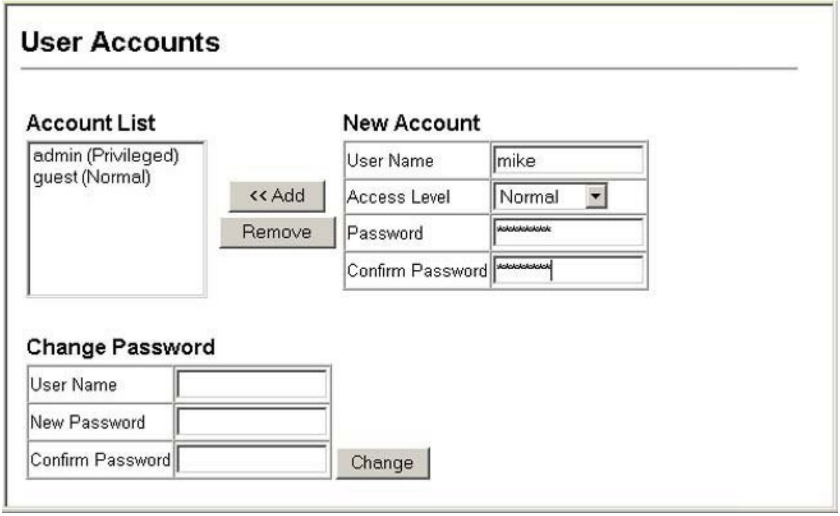
The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. You should therefore assign a new administrator password as soon as possible, and store it in a safe place.

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.”

Command Attributes

- **Account List** – Displays the current list of user accounts and associated access levels. (Defaults: admin, and guest)
- **New Account** – Displays configuration settings for a new account.
  - **User Name** – The name of the user.
    (Maximum length: 8 characters; maximum number of users: 16)
  - **Access Level** – Specifies the user level.
    (Options: Normal and Privileged)
  - **Password** – Specifies the user password.
    (Range: 0-8 characters plain text, case sensitive)
- **Change Password** – Sets a new password for the specified user.

Web – Click Security, User Accounts. To configure a new user account, enter the user name, access level, and password, then click Add. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again, then click Apply.



User Accounts

Account List

admin (Privileged)
guest (Normal)

New Account

User Name	mike
Access Level	Normal
Password	********
Confirm Password	********

Change Password

User Name	
New Password	
Confirm Password	

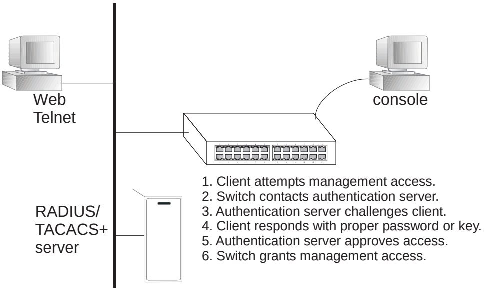
Figure 6-1 User Accounts

CLI – Assign a user name to access-level 15 (i.e., administrator), then specify the password.

```
Console(config)#username bob access-level 15                      25-2
Console(config)#username bob password 0 smith
Console(config)#
```

Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. You can manually configure access rights on the switch, or you can use a remote access authentication server based on RADIUS or TACACS+ protocols.



1. Client attempts management access.
2. Switch contacts authentication server.
3. Authentication server challenges client.
4. Client responds with proper password or key.
5. Authentication server approves access.
6. Switch grants management access.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS- aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the switch.

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local switch. If a remote authentication server is used, you must specify the authentication sequence and the corresponding parameters for the remote authentication protocol. Local and remote logon authentication control management access via the console port, web browser, or Telnet.
- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify up to three authentication methods for any user to indicate the authentication sequence. For example, if you select (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

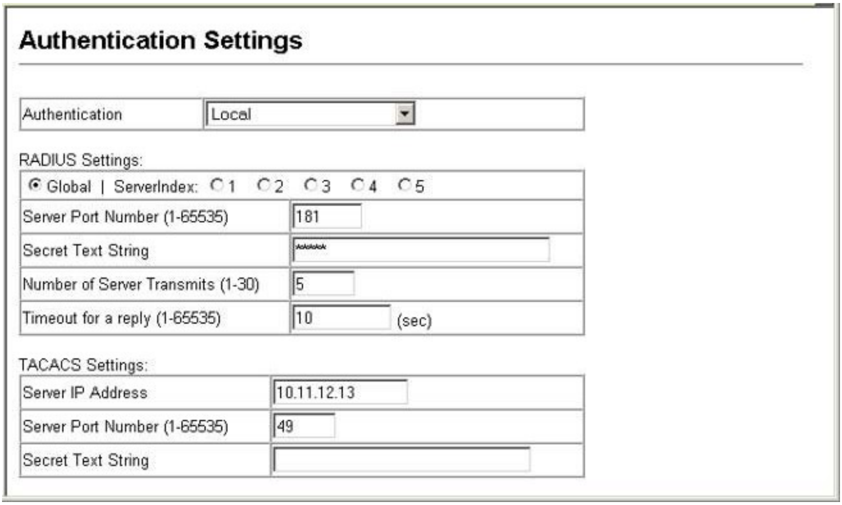
Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
  - **Local** – User authentication is performed only locally by the switch.
  - **Radius** – User authentication is performed using a RADIUS server only.
  - **TACACS** – User authentication is performed using a TACACS+ server only.
  - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.
- **RADIUS Settings**
  - **Global** – Provides globally applicable RADIUS settings.
  - **Server Index** – Specifies one of five RADIUS servers that may be configured. The switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
  - **Server IP Address** – Address of authentication server. (Default: 10.1.0.1)
  - **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
  - **Number of Server Transmits** – Number of times the switch tries to authenticate logon access via the authentication server. (Range: 1-30; Default: 2)
  - **Timeout for a reply** – The number of seconds the switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)

- **TACACS Settings**
  - **Server IP Address** – Address of the TACACS+ server. (Default: 10.11.12.13)
  - **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
  - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Note: The local switch user database has to be set up by manually entering user names and passwords using the CLI. (See “username” on page 25-2.)

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (i.e., one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.



Authentication Settings

Authentication	Local

RADIUS Settings:

● Global | ServerIndex: ○1 ○2 ○3 ○4 ○5	
Server Port Number (1-65535)	181
Secret Text String	******
Number of Server Transmits (1-30)	5
Timeout for a reply (1-65535)	10 (sec)

TACACS Settings:

Server IP Address	10.11.12.13
Server Port Number (1-65535)	49
Secret Text String	

Figure 6-2 Authentication Server Settings

CLI – Specify all the required parameters to enable logon authentication.

```
Console(config)#authentication login radius                          25-4
Console(config)#radius-server port 181                               25-7
Console(config)#radius-server key green                              25-7
Console(config)#radius-server retransmit 5                           25-8
Console(config)#radius-server timeout 10                             25-8
Console(config)#radius-server 1 host 192.168.1.25                    25-9
Console(config)#exit
```

```
Console#show radius-server                                           25-8

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   181
 Retransmit times:                     5
 Request timeout:                      10

Server 1:
 Server IP address: 192.168.1.25
 Communication key with RADIUS server: *****
 Server port number: 181
 Retransmit times: 5
 Request timeout: 10

Console#config
Console(config)#authentication login tacacs                          25-4
Console(config)#tacacs-server host 10.20.30.40                       25-9
Console(config)#tacacs-server port 200                               25-10
Console(config)#tacacs-server key green                              25-10
Console(config)#exit
Console#show tacacs-server                                           25-11
Server IP address:                      10.20.30.40
 Communication key with tacacs server: *****
 Server port number:                   200
Console(config)#
```

Configuring HTTPS

You can configure the switch to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure both services to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: https://*device*[:*port_number*]
- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
  A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape 6.2 or above.

- The following web browsers and operating systems currently support HTTPS:

Table 6-1 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see “Replacing the Default Secure-site Certificate” on page 6-7.

Command Attributes

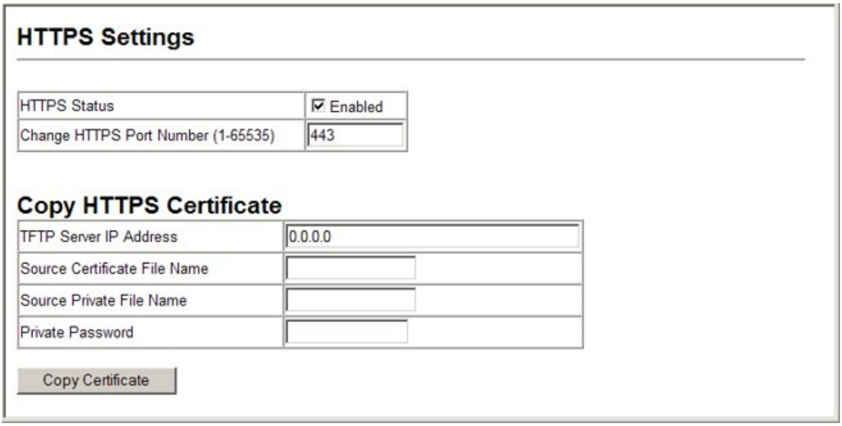
HTTPS Settings

- **HTTPS Status** – Allows you to enable/disable the HTTPS server feature on the switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/ SSL connection to the switch’s web interface. (Default: Port 443)

Copy HTTPS Certificate

For more information on this function, see “Replacing the Default Secure-site Certificate” on page 6-7.

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.



HTTPS Settings

HTTPS Status	☑ Enabled
Change HTTPS Port Number (1-65535)	443

Copy HTTPS Certificate

TFTP Server IP Address	0.0.0.0
Source Certificate File Name	
Source Private File Name	
Private Password	

Figure 6-3 HTTPS Settings

CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server                                     25-12
Console(config)#ip http secure-port 441                                   25-13
Console(config)#
```

Replacing the Default Secure-site Certificate

When you log onto the web interface using HTTPS (for secure access), a Secure Sockets Layer (SSL) certificate appears for the switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. If you want this warning to be replaced by a message confirming that the connection to the switch is secure, you must obtain a unique certificate and a private key and password from a recognized certification authority.

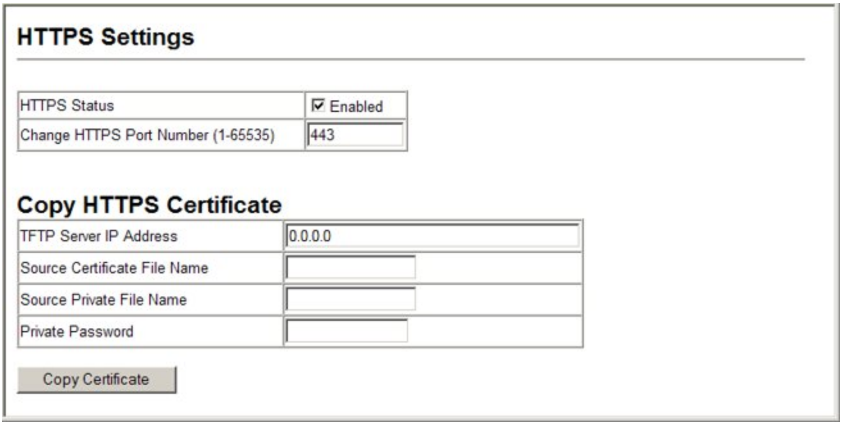
Note: For maximum security, we recommend you obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the switch is not unique to the hardware you have purchased.

When you have obtained these, place them on your TFTP server and transfer them to the switch to replace the default (unrecognized) certificate with an authorized one.

Command Attributes

- **TFTP Server IP Address** – IP address of TFTP server which contains the certificate file.
- **Source Certificate File Name** – Name of certificate file stored on the TFTP server.
- **Source Private File Name** – Name of private key file stored on the TFTP server.
- **Private Password** – Password stored in the private key file. This password is used to verify authorization for certificate use, and is verified when downloading the certificate to the switch.

Web – Click Security, HTTPS Settings. Fill in the TFTP server, certificate and private file name details, then click Copy Certificate.



HTTPS Settings

HTTPS Status	☑ Enabled
Change HTTPS Port Number (1-65535)	443

Copy HTTPS Certificate

TFTP Server IP Address	0.0.0.0
Source Certificate File Name	
Source Private File Name	
Private Password	

Figure 6-4 HTTPS Settings

CLI – This example copies the certificate file from the designated TFTP server.

```
Console#copy tftp https-certificate                                    23-11
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The switch must be reset for the new certificate to be activated. To reset the switch, type “reload” at the command prompt: `Console#reload`

Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to this switch as a secure replacement for Telnet. When the client contacts the switch via the SSH protocol, the switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that you need to install an SSH client on the management station to access the switch for management via the SSH protocol.

Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Command Usage

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified on the **Authentication Settings** page (page 6-2). If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.

2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management

station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
15020245593199868544358361651999923329781766065830956 10825913212890233
76546801726272571413428762941301196195566782 59566410486957427888146206
519417467729848654686157177393901647793559423035774130980227370877945452
4083971752646358058176716709574804776117
```

3. *Import Client’s Public Key to the Switch* – Use the **copy tftp public-key** command (page 23-11) to copy a file containing the public key for all the SSH client’s granted management access to the switch. (Note that these clients must be configured locally on the switch via the User Accounts page as described on page 6-1.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

```
1024 35 1341081685609893921040944920155425347631641921872958921143173880
055536161631051775940838686311092912322268285192543746031009371877211996
963178136627741416898513204911720483033925432410163799759237144901193800
609025394840848271781943722884025331159521348610229029789827213532671316
29432532818915045306393916643 steve@192.168.1.19
```

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the switch.

6. *Authentication* – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

   Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client’s keys.

   Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

   Authenticating SSH v1.5 Clients

   a. The client sends its RSA public key to the switch.
   b. The switch compares the client's public key to those stored in memory.
   c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user’s public key, and sends it to the client.

d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.

e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.

b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

c. The client sends a signature generated using the private key to the switch.

d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the switch. After generating this key pair, you must provide the host public key to SSH clients and import the client’s public key to the switch as described in the preceding section (Command Usage).

Field Attributes

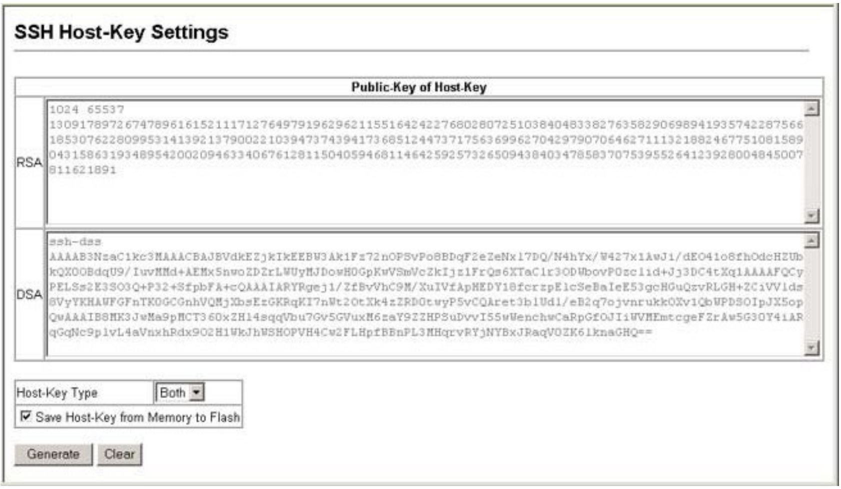
- **Public-Key of Host-Key** – The public key for the host.
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 65537), and the last string is the encoded modulus.
  - DSA: The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- **Host-Key Type** – The key type used to generate the host key pair (i.e., public and private keys). (Range: RSA, DSA, Both: Default: Both)

  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

Note: The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (i.e., volatile memory to flash memory). Otherwise, the host key pair is stored to RAM by default. Note that you must select this item prior to generating the host-key pair.
- **Generate** – This button is used to generate the host key pair. Note that you must first generate the host key pair before you can enable the SSH server on the SSH Server Settings page.
- **Clear** – This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

Web – Click Security, SSH, Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click Generate.



SSH Host-Key Settings

Public-Key of Host-Key

RSA

```
1024 65537
13091789726747896161521117127649791962962115516424227680280725103840483382763582906989419357422875661
85307622809953141392137900221039473743941736851244737175636996270429790706462711113218824677510815890
43158631934895420020946334067612811504059468114642592573265094384034785837075395526412392800484500781
1621891
```

DSA

```
ssh-dss
AAAAB3NzaC1kc3MAAACBAJBVdkEZjkIkEEBW3Ak1Fz72nOPSvPo8BDqF2eZeNx17DQ/N4hYx/W427x1AwJi/dEO41o8fhOdcHZUb
kQXOOBdqU9/IuvMMd+AEMx5nwoZDZrLWUyMJDowHOGpKwVSmVcZkIjz1FrQs6XTaC1r3ODWbovPOzc1id+Jj3DC4tXq1AAAAFQCy
PELSs2E3SO3Q+P32+SfpbFA+cQAAAIARYRgej1/ZfBvVhC9M/XuIVfApMEDY18fcrzpE1cSeBaIeE53gcHGuQzvRLGH+ZCiVV1ds
8VyYKHAWFGFnTKOGCGnhVQMjXbsEzGKRqKI7nWt2OtXk4zZRDOtwyP5vCQAret3b1Ud1/eB2q7ojvnrukkOXv1QbWPDSOIpJX5op
QwAAAIB8MK3JwMa9pMCT360xZH14sqqVbu7Gv5GVuxM6zaY9ZZHPSuDvvI55wWenchwCaRpGfOJIiWVMEmtcgeFZrAw5G3OY4iAR
qGqNc9plvL4aVnxhRdx9O2H1WkJhWSHOPVH4Cw2FLHpfBBnPL3MHqrvRYjNYBxJRaqVOZK61knaGHQ==
```

Host-Key Type	Both

☑ Save Host-Key from Memory to Flash

Figure 6-5 SSH Host-Key Settings

CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```
Console#ip ssh crypto host-key generate                               25-20
Console#ip ssh save host-key                                          25-21
Console#show public-key host                                          25-23
Host:
RSA:
1024 65537 127250922544926402131336514546131189679055192360076028653006761
824096909474483201025248789659775921683222255846523877915464798073963140330
869257931051057652122430528078658854857892726029378660892368414232759121277
603259196836970534393364384452233351882871738968945117292905108139196420255
1909321043285790457648 91
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasfEthIwmj
hLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIICuKg6vjO9XTs7XKc05xfzkBi
KviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6DkZAAAAFQCNZn/x17dwpW8RrV
DQnSWw4Qk+6QAAAIEAptkGeB6B5hwagH4gUOCY6i1TmrmSiJgfwO9OqRPUMbCAkCC+uzxatOo7
drnIZypMx+Sx5RUdMGgKS+9ywsa1cWqHeFY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLG
Nq375R55yRxFvmcGIn/Q7IphPqyJ3o9MK8LFDfmJEAAACAL8A6tESiswP2OFqX7VGoEbzVDSOI
RTMFy3iUXtvGyQAOVSy67Mfc3lMtgqPRUOYXDiwIBp5NXgilCg5z7VqbmRm28mWc5a//f8TUAg
PNWKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5Kytdn4MdoTHgrbl/DMdAfjnte8MZZs=

Console#
```

Importing User Public Keys

A user's Public Key must be uploaded to the switch in order for the user to be able to log in using the public key authentication mechanism. If the user's public key does not exist on the switch, SSH will revert to the interactive password authentication mechanism to complete authentication.

Field Attributes

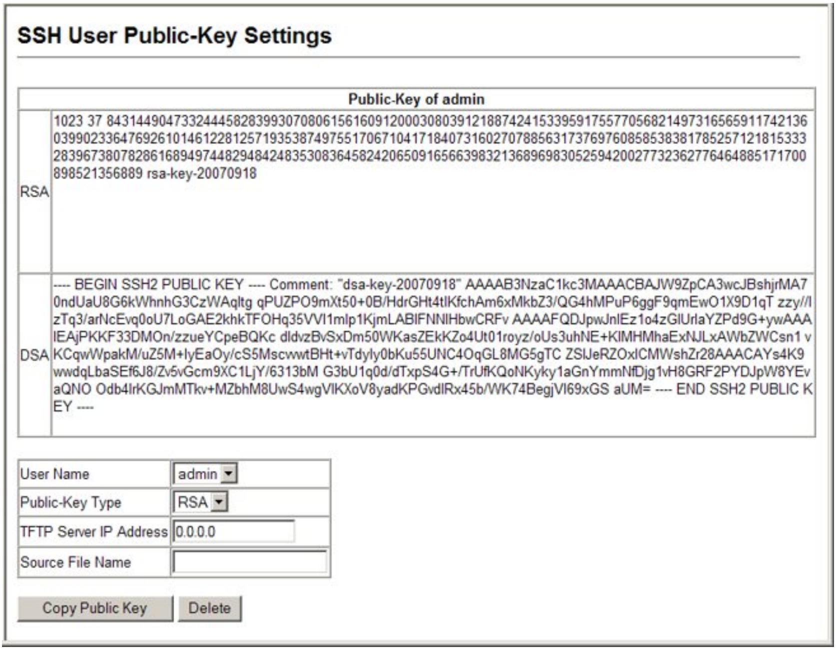
- **Public-Key of *user*** – The RSA and DSA public keys for the selected user.
  - RSA: The first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 37), and the last string is the encoded modulus.
  - DSA: The first field indicates that SSH version 2 was used to create the key. The second field contains the key comment. The third string is the encoded modulus, and the last field is a comment denoting the end of the key.
- **User Name** – This drop-down box selects the user who's public key you wish to manage. Note that you must first create users on the User Accounts page (See "Configuring User Accounts" on page 6-1.).
- **Public-Key Type** – The type of public key to upload.
  - RSA: The switch accepts a RSA version 1 encrypted public key.
  - DSA: The switch accepts a DSA version 2 encrypted public key.

  The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

  The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.

- **TFTP Server IP Address** – The IP address of the TFTP server that contains the public key file you wish to import. (Default: 0.0.0.0)
- **Source File Name** – The public key file to upload.
- **Copy Public Key** – Initiates the public key TFTP import process. If you are replacing an outdated public key file, it is not necessary to first delete the original key from the switch. The import process will overwrite the existing key.
- **Delete** – Deletes a selected RSA or DSA public key that has already been imported to the switch.

Web – Click Security, SSH, SSH User Public-Key Settings. Select the user name and the public-key type from the respective drop-down boxes, input the TFTP server IP address and the public key source file name, and then click Copy Public Key.



SSH User Public-Key Settings

Public-Key of admin	
RSA	1023 37 843144904733244458283993070806156160912000308039121887424153395917557705682149731656591174213603990233647692610146122812571935387497551706710417184073160270788563173769760858538381785257121815333283967380782861689497448294842483530836458242065091656639832136896983052594200277323627764648851717008985213568889 rsa-key-20070918
DSA	---- BEGIN SSH2 PUBLIC KEY ---- Comment: "dsa-key-20070918" AAAAB3NzaC1kc3MAAACBAJW9ZpCA3wcJBshjrMA70ndUaU8G6kWhnhG3CzWAqltg qPUZPO9mXt50+0B/HdrGHt4tIKfchAm6xMkbZ3/QG4hMPuP6ggF9qmEwO1X9D1qT zzy//IzTq3/arNcEvq0oU7LoGAE2khkTFOHq35VVI1mIp1KjmLABIFNNIHbwCRFv AAAAFQDJpwJnlEz1o4zGlUrlaYZPd9G+ywAAAlEAjPKKF33DMOn/zzueYCpeBQKc dldvzBvSxDm50WKasZEkKZo4Ut01royz/oUs3uhNE+KIMHMhaExNJLxAWbZWCsn1 vKCqwWpakM/uZ5M+lyEaOy/cS5MscwwtBHt+vTdyly0bKu55UNC4OqGL8MG5gTC ZSlJeRZOxICMWshZr28AAACAYs4K9wwdqLbaSEf6J8/Zv5vGcm9XC1LjY/6313bM G3bU1q0d/dTxpS4G+/TrUfKQoNKyky1aGnYmmNfDjg1vH8GRF2PYDJpW8YEvaQNO Odb4IrKGJmMTkv+MZbhM8UwS4wgVIKXoV8yadKPGvdlRx45b/WK74BegjVI69xGS aUM= ---- END SSH2 PUBLIC KEY ----

User Name	admin
Public-Key Type	RSA
TFTP Server IP Address	0.0.0.0
Source File Name	

Figure 6-6 SSH User Public-Key Settings

CLI – This example imports an SSHv2 DSA public key for the user admin and then displays admin’s imported public keys. Note that public key authentication through SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key                                            23-11
TFTP server IP address: 192.168.1.254
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 2
Source file name: admin-ssh2-dsa-pub.key
Username: admin
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#show public-key user admin                                      25-23
admin:
RSA:
1024 37 154886675541099600242673908076171863880953984597454546825066951007
29617437427136900505591624068119579408716226078634780682201498685790475062
34519480679939485042653504179153032795337422103356695026441903823445835730
88823472889690842821665429031315937652815279387868298539820466143474130023
09979848162607182657 rsa-key-20071106

DSA:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20071105"
AAAAB3NzaC1kc3MAAA
CAeqNnwpAVz82Z3zFif0KGF846S5m5useW8rQp8DBv1IQ/sLYRuoCtW/+hllIaUu2F9Ps6D5gJ
dKjyEPKRutJv1rAwq1YZ61/fat9OGpM3oaqMf6UiVUK4gEsaq8T6UqrGsIDcXWyvmbI02+R/
owN43kwEJCfmpBXelhU962AA2G0AAAAVAKxtZo+MjTVzRJ+9mFTFIUpawm7HAAAAgCINbco4jT
WcdMKS1oQTA+WnCehlsd8j5MpDc3VccySMaFzcPgxT+N79WVxWNJQaS8l9TfY3EDg9VfCooLZD
rn/yX67MV3p/IJej57DsNjLnCHpaGE/OKfkAhvjRzlufS4f4wAzOYCBNxb6XY6Vew8Pi7Wri
L/Xrm4AQ0t4wSjjEAAAAgDNcKKEpZw16wW7E9EmbQp5s5gu9lCVCqMz5r76EyEzc
9uIYvxy54GHMtyBwLTITh6lbxEGD6cOnkCW+ieRye9fiJfs7u4QdL9NZb+WLZvcUXm6E1vUc70
OpelDFxbfhQawgGFxvx7rzv85D75ffNEqbLW2mKApehuQrHYbPZOnX
---- END SSH2 PUBLIC KEY ----


Console#
```

Configuring the SSH Server

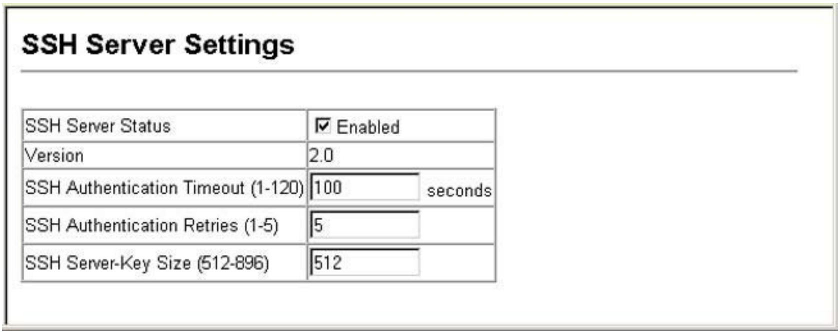
The SSH server includes basic settings for authentication.

Field Attributes

- **SSH Server Status** – Allows you to enable/disable the SSH server on the switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the switch supports management access via either SSH Version 1.5 or 2.0 clients.
- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt. (Range: 1 to 120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)

- **SSH Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default: 768)
  - The server key is a private key that is never shared outside the switch.
  - The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that you must first generate the host key pair on the SSH Host-Key Settings page before you can enable the SSH server.



SSH Server Settings

SSH Server Status	☑ Enabled
Version	2.0
SSH Authentication Timeout (1-120)	100 seconds
SSH Authentication Retries (1-5)	5
SSH Server-Key Size (512-896)	512

Figure 6-7 SSH Server Settings

CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection via SHH, and then disables this connection.

```
Console(config)#ip ssh server                                         25-17
Console(config)#ip ssh timeout 100                                    25-18
Console(config)#ip ssh authentication-retries 5                       25-19
Console(config)#ip ssh server-key size 512                            25-19
Console(config)#end
Console#show ip ssh                                                   25-22
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh                                                      25-22
Information of secure shell
Session Username Version Encrypt method Negotiation state
------- -------- ------- -------------- -----------------
      0     admin    2.0       cipher-3des    session-started
Console#disconnect 0                                                  23-24
Console#
```

Configuring Port Security

Port security is a feature that allows you to configure a switch port with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (page 9-1). When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

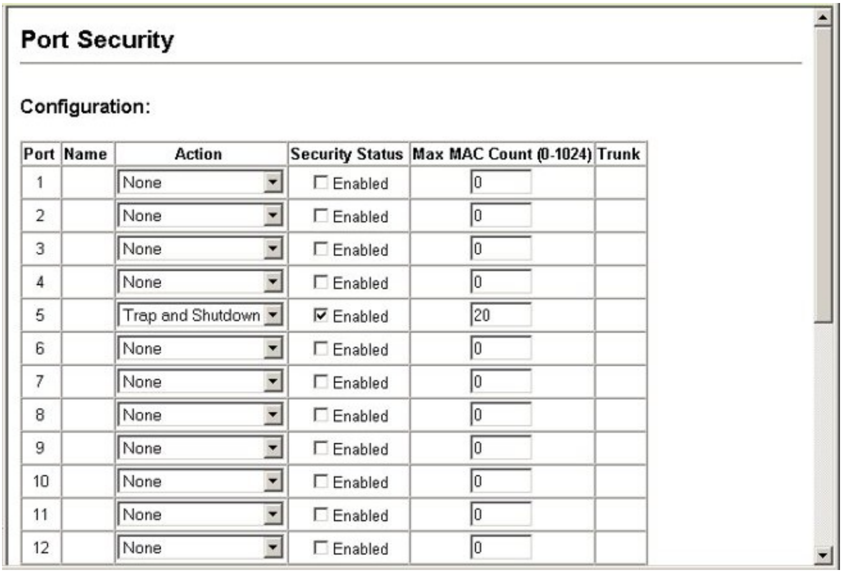
Command Usage

- A secure port has the following restrictions:
  - It cannot be used as a member of a static or dynamic trunk.
  - It should not be connected to a network interconnection device.
- The default maximum number of MAC addresses allowed on a secure port is zero. You must configure a maximum address count from 1 - 1024 for the port to allow access.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (page 8-3).

Command Attributes

- **Port** – Port number.
- **Name** – Descriptive text (page 27-2).
- **Action** – Indicates the action to be taken when a port security violation is detected:
  - **None**: No action should be taken. (This is the default.)
  - **Trap**: Send an SNMP trap message.
  - **Shutdown**: Disable the port.
  - **Trap and Shutdown**: Send an SNMP trap message and disable the port.
- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)
- **Trunk** – Trunk number if port is a member (page 8-7 and 8-8).

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, mark the checkbox in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port, and click Apply.



Port Security

Configuration:

Port	Name	Action	Security Status	Max MAC Count (0-1024)	Trunk
1		None	☐ Enabled	0	
2		None	☐ Enabled	0	
3		None	☐ Enabled	0	
4		None	☐ Enabled	0	
5		Trap and Shutdown	☑ Enabled	20	
6		None	☐ Enabled	0	
7		None	☐ Enabled	0	
8		None	☐ Enabled	0	
9		None	☐ Enabled	0	
10		None	☐ Enabled	0	
11		None	☐ Enabled	0	
12		None	☐ Enabled	0	

Figure 6-8 Port Security

CLI – This example selects the target port, sets the port security action to send a trap and disable the port, specifies a maximum address count, and then enables port security for the port.

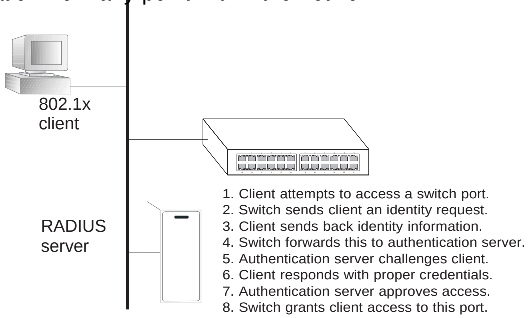
```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown         25-25
Console(config-if)#port security max-mac-count 20
Console(config-if)#port security
Console(config-if)#
```

Configuring 802.1X Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (i.e., Supplicant) connects to a switch port, the switch (i.e., Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method must be MD5. (TLS, TTLS and PEAP will be supported in future releases.) The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.



1. Client attempts to access a switch port.
2. Switch sends client an identity request.
3. Client sends back identity information.
4. Switch forwards this to authentication server.
5. Authentication server challenges client.
6. Client responds with proper credentials.
7. Authentication server approves access.
8. Switch grants client access to this port.

The operation of dot1x on the switch requires the following:

- The switch must have an IP address assigned.
- The IP address of the RADIUS server must be specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to dot1x “Auto” mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The switch only supports EAPOL in order to pass the EAP packets from the server to the client.)

- The RADIUS server and client also have to support the same EAP authentication type – MD5. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

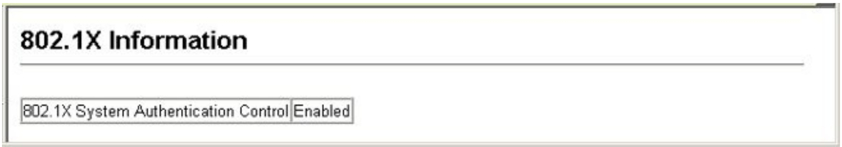
Displaying 802.1X Global Settings

The 802.1X protocol provides port authentication.

Command Attributes

802.1X System Authentication Control – The global setting for 802.1X.

Web – Click Security, 802.1X, Information.



802.1X Information

802.1X System Authentication Control Enabled

Figure 6-9 802.1X Global Information

CLI – This example shows the default global setting for 802.1X.

```
Console#show  dot1x                                                        25-32
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name   Status           Operation Mode    Mode                  Authorized
1/1          disabled        Single-Host       ForceAuthorized       n/a
1/2          disabled        Single-Host       ForceAuthorized       n/a
:
802.1X Port Details

802.1X is disabled on port 1/1
:
802.1X is disabled on port 26
Console#
```

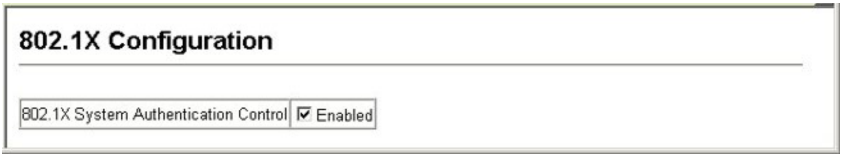
Configuring 802.1X Global Settings

The 802.1X protocol provides port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

Command Attributes

802.1X System Authentication Control – Sets the global setting for 802.1X. (Default: Disabled)

Web – Select Security, 802.1X, Configuration. Enable 802.1X globally for the switch, and click Apply.



802.1X Configuration

802.1X System Authentication Control ☑ Enabled

Figure 6-10 802.1X Global Configuration

CLI – This example enables 802.1X globally for the switch.

```
Console(config)#dot1x system-auth-control                          25-27
Console(config)#
```

Configuring Port Settings for 802.1X

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (i.e., authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port. (Default: Disabled)
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host, MAC-Based; Default: Single-Host)
  - In Single-Host mode, only one host connected to a port can be authenticated for network access.
  - In Multi-Host mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message. The number of hosts allowed access to a port operating in this mode is determined by the Max Count attribute described below.
  - In MAC-Based mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

- **Max Count** – The maximum number of hosts that can connect to a port when the operation mode is set to Multi-Host. (Range: 1-1024; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
  - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
  - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
  - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.

  802.1X port authentication and port security (page 6-16) cannot be configured together on the same port. Only one of these security mechanisms can be applied.

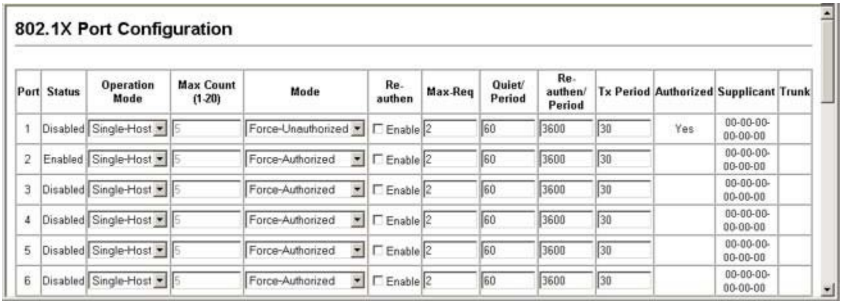
  802.1X port authentication cannot be configured on trunk ports. In other words, a static or dynamically configured trunk cannot be set to Auto or Force-Unauthorized mode.

  When 802.1X authentication is enabled on a port, the MAC address learning function for this interface is disabled, and the addresses dynamically learned on this port are removed.

  Authenticated MAC addresses are stored as dynamic entries in the switch's secure MAC address table. Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.

  When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.
- **Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. (Default: Disabled)
- **Max Request** – Sets the maximum number of times the switch port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Quiet Period** – Sets the time that a switch port waits after the Max Request count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **TX Period** – Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Authorized** –
  - **Yes** – Connected client is authorized.
  - **No** – Connected client is not authorized.
  - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1X, Port Configuration. Modify the parameters required, and click Apply.



802.1X Port Configuration

Port	Status	Operation Mode	Max Count (1-20)	Mode	Re-authen	Max-Req	Quiet/ Period	Re-authen/ Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Unauthorized	☐ Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
2	Enabled	Single-Host	5	Force-Authorized	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authorized	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authorized	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authorized	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authorized	☐ Enable	2	60	3600	30		00-00-00-00-00-00	

Figure 6-11 802.1X Port Configuration

CLI – This example sets the 802.1X parameters on port 2. For a description of the additional fields displayed in this example, see “show dot1x” on page 25-32.

```
Console(config)#interface ethernet 1/2                              27-1
Console(config-if)#dot1x port-control auto                         25-28
Console(config-if)#dot1x re-authentication                         25-30
Console(config-if)#dot1x max-req 5                                 25-27
Console(config-if)#dot1x timeout quiet-period 40                   25-31
Console(config-if)#dot1x timeout re-authperiod 5                   25-31
Console(config-if)#dot1x timeout tx-period 40                      25-32
Console(config-if)#end
Console#show dot1x                                                 25-32

Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status         Operation Mode   Mode                Authorized
1/1        disabled       Single-Host       ForceAuthorized    yes
1/2        enabled        Single-Host      Auto                yes
:
1/25       disabled        Single-Host      ForceAuthorized    n/a
1/26       disabled        Single-Host      ForceAuthorized    n/a


802.1X Port Details


802.1X is disabled on port 1/1

802.1X is enabled on port 1/2
reauth-enabled:         Disable
reauth-period:          3600
quiet-period:           60
tx-period:              30
supplicant-timeout:     30
server-timeout:         10
reauth-max:             2
max-req:                2
Status                   Authorized
Operation mode           Single-Host
Max count               5
Port-control            Auto
Supplicant               00-e0-29-94-34-65
Current Identifier      7

Authenticator State Machine
State                    Authenticated
Reauth Count            0

Backend State Machine
State                   Idle
Request Count           0
Identifier(Server)      6

Reauthentication State Machine
State                    Initialize
:
802.1X is disabled on port 1/26
Console#
```

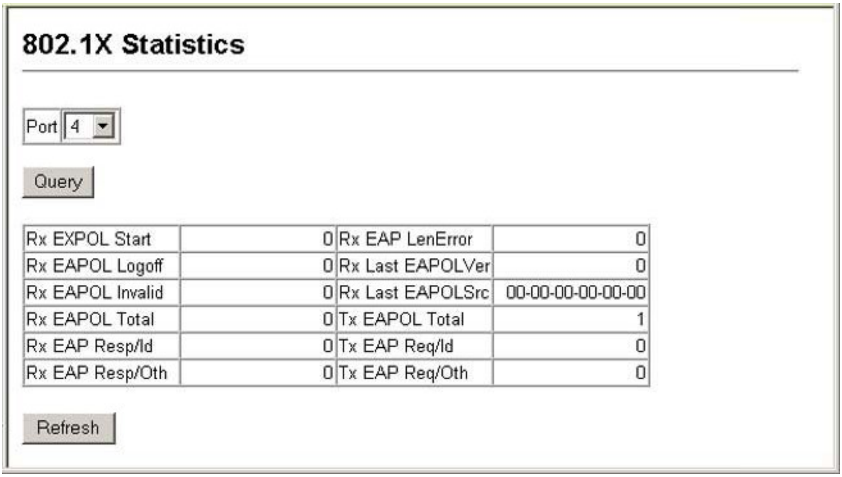
Displaying 802.1X Statistics

This switch can display statistics for dot1x protocol exchanges for any port.

Table 6-2 802.1X Statistics

Parameter	Description
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select Security, 802.1X, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.



802.1X Statistics

Port 4

Rx EXPOL Start	0	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	0
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-00-00-00-00
Rx EAPOL Total	0	Tx EAPOL Total	1
Rx EAP Resp/Id	0	Tx EAP Req/Id	0
Rx EAP Resp/Oth	0	Tx EAP Req/Oth	0

Figure 6-12 802.1X Port Statistics

CLI – This example displays the dot1x statistics for port 4.

```
Console#show dot1x statistics interface ethernet 1/4                     25-32

Eth 1/4
Rx: EAPOL       EAPOL       EAPOL       EAPOL       EAP       EAP       EAP
    Start        Logoff     Invalid      Total     Resp/Id   Resp/Oth LenError
        2           0           0        1007       672         0         0

    Last       Last
EAPOLVer      EAPOLSrc
       1       00-00-E8-98-73-21

Tx: EAPOL       EAP       EAP
    Total      Req/Id    Req/Oth
     2017      1005         0
Console#
```

Filtering IP Addresses for Management Access

You can create a list of up to 16 IP addresses or IP address groups that are allowed management access to the switch through the web interface, SNMP, or Telnet.

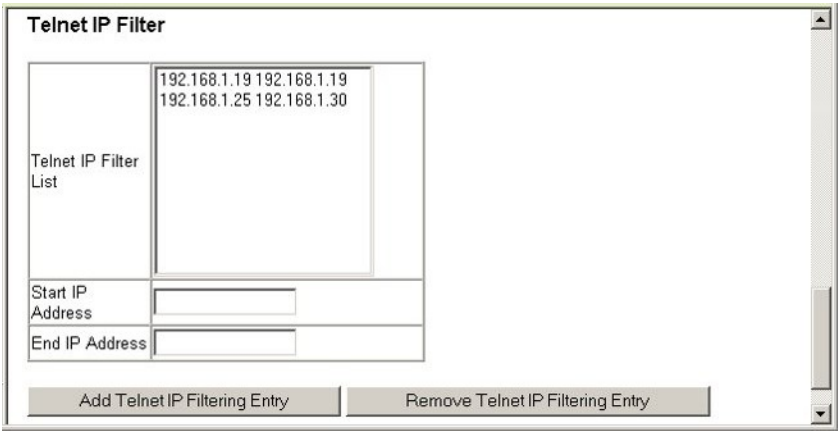
Command Usage

- The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **IP Filter List** – IP address which are allowed management access to this interface.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

Web – Click Security, IP Filter. Enter the IP addresses or range of addresses that are allowed management access to an interface, and click Add IP Filtering Entry.



Telnet IP Filter

Telnet IP Filter List	192.168.1.19 192.168.1.19 192.168.1.25 192.168.1.30
Start IP Address	
End IP Address	

Add Telnet IP Filtering Entry
Remove Telnet IP Filtering Entry

Figure 6-13 IP Filter

CLI – This example restricts management access for Telnet clients.

```
Console(config)#management telnet-client 192.168.1.19                   25-35
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console(config)#exit
Console#show management all-client                                     25-36
Management IP Filter
 HTTP-Client:
   Start IP address        End IP address
-----------------------------------------------

 SNMP-Client:
   Start IP address        End IP address
-----------------------------------------------

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#
```

Chapter 7: Access Control Lists

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, next header type, or flow label), or any frames (based on MAC address or Ethernet type). To filter incoming packets, first create an access list, add the required rules, and then bind the list to a specific port.

Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. This switch tests ingress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match, the packet is accepted.

Command Usage

The following restrictions apply to ACLs:

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32.
- The maximum number of rules that can be bound to the ports is 96 for each of the following list types: MAC ACLs, IP ACLs (including Standard and Extended ACLs), IPv6 Standard ACLs, and IPv6 Extended ACLs. For the IC40240-10G, all ports share this quota. For the IC40480-10G, ports 1-24 share a quota of 96 rules, and ports 25-50 share another quota of 96 rules (since there are two switch chips in this system).

The order in which active ACLs are checked is as follows:

1. User-defined rules in IP and MAC ACLs for ingress ports are checked in parallel.
2. Rules within an ACL are checked in the configured order, from top to bottom.
3. If the result of checking an IP ACL is to permit a packet, but the result of a MAC ACL on the same packet is to deny it, the packet will be denied (because the decision to deny a packet has a higher priority for security reasons). A packet will also be denied if the IP ACL denies it and the MAC ACL accepts it.

Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

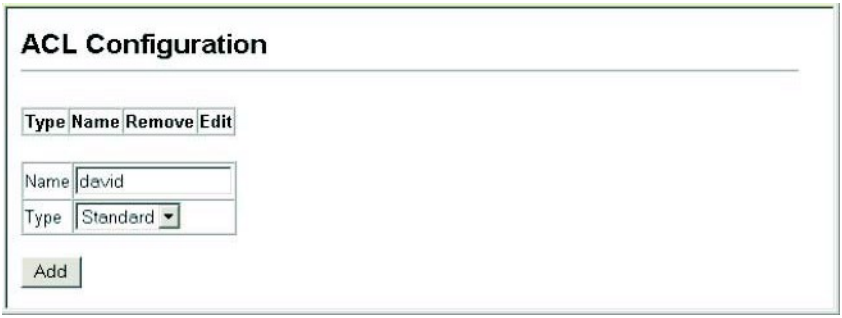
Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
  - **IP Standard**: IPv4 ACL mode that filters packets based on the source IPv4 address.
  - **IP Extended**: IPv4 ACL mode that filters packets based on source or destination IPv4 address, as well as protocol type and protocol port number.

If the “TCP” protocol is specified, then you can also filter packets based on the TCP control code.

- **IPv6 Standard**: IPv6 ACL mode that filters packets based on the source IPv6 address.
- **IPv6 Extended**: IPv6 ACL mode that filters packets based on the destination IP address, as well as the type of the next header and the flow label (i.e., a request for special handling by IPv6 routers).
- **MAC**: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click Security, ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, MAC, IPv6 Standard, IPv6 Extended), and click Add to open the configuration page for the new list.



ACL Configuration

Type	Name	Remove	Edit

Name	david
Type	Standard

Figure 7-1 Selecting ACL Type

CLI – This example creates a standard IP ACL named bill.

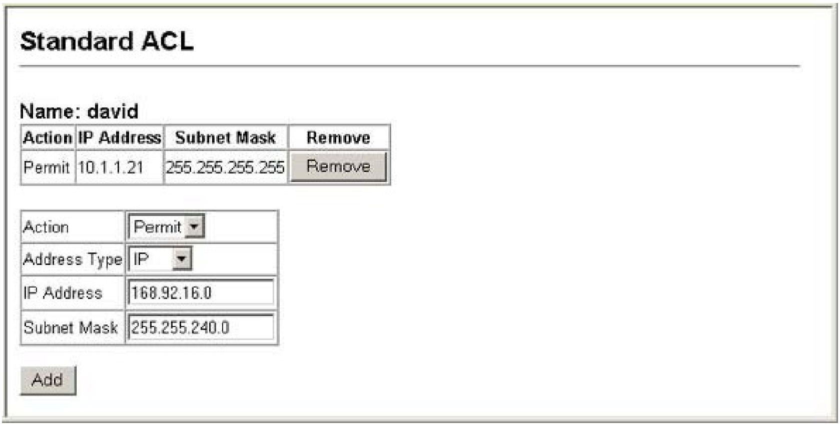
```
Console(config)#access-list ip standard bill                         26-2
Console(config-std-acl)#
```

Configuring a Standard IPv4 ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **IP Address** – Source IP address.
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Then click Add.



Standard ACL

Name: david

Action	IP Address	Subnet Mask	Remove
Permit	10.1.1.21	255.255.255.255	Remove

Action	Permit
Address Type	IP
IP Address	168.92.16.0
Subnet Mask	255.255.240.0

Figure 7-2 ACL Configuration - Standard IPv4

CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21                       26-2
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Configuring an Extended IPv4 ACL

Command Attributes

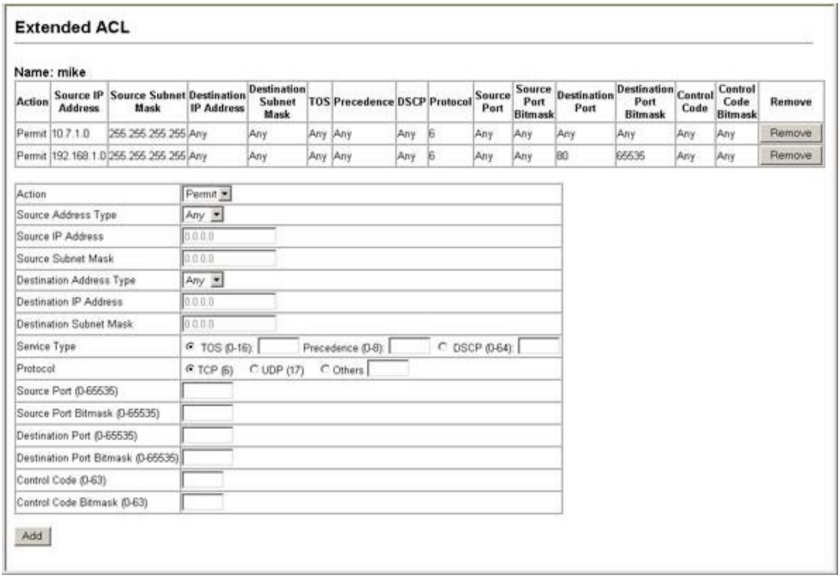
- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.
- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 2.)
- **Service Type** – Packet priority settings based on the following criteria:
  - **Precedence** – IP precedence level. (Range: 0-7)
  - **TOS** – Type of Service level. (Range: 0-15)
  - **DSCP** – DSCP priority level. (Range: 0-63)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)

- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bit Mask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bit Mask** – Decimal number representing the code bits to match. The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:

  - SYN flag valid, use control-code 2, control bitmask 2
  - Both SYN and ACK valid, use control-code 18, control bitmask 18
  - SYN valid and ACK invalid, use control-code 2, control bitmask 18

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or IP). If you select “Host,” enter a specific address. If you select “IP,” enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.



Extended ACL

Name: mike

Action	Source IP Address	Source Subnet Mask	Destination IP Address	Destination Subnet Mask	TOS	Precedence	DSCP	Protocol	Source Port	Source Port Bitmask	Destination Port	Destination Port Bitmask	Control Code	Control Code Bitmask	Remove
Permit	10.7.1.0	255.255.255.255	Any	Any	Any	Any	Any	6	Any	Any	Any	Any	Any	Any	Remove
Permit	192.168.1.0	255.255.255.255	Any	Any	Any	Any	Any	6	Any	Any	80	65535	Any	Any	Remove

Action	Permit
Source Address Type	Any
Source IP Address	0.0.0.0
Source Subnet Mask	0.0.0.0
Destination Address Type	Any
Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Service Type	● TOS (0-16): Precedence (0-8): ○ DSCP (0-64):
Protocol	● TCP (6) ○ UDP (17) ○ Others
Source Port (0-65535)	
Source Port Bitmask (0-65535)	
Destination Port (0-65535)	
Destination Port Bitmask (0-65535)	
Control Code (0-63)	
Control Code Bitmask (0-63)	

Figure 7-3 ACL Configuration - Extended IPv4

CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).
3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any        26-3
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
  control-flag 2 2
Console(config-std-acl)#
```

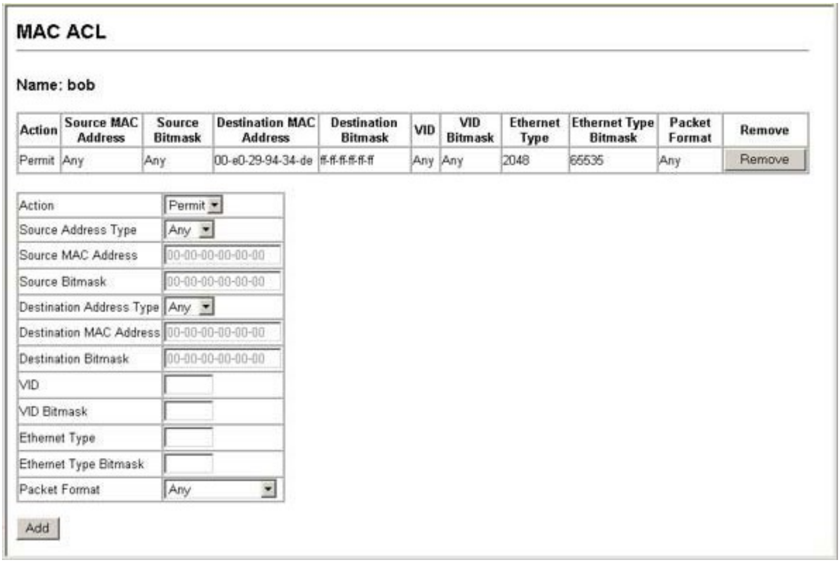
Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source/Destination** Address Type – Use “Any” to include all possible addresses, “Host” to indicate a specific MAC address, or “MAC” to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination MAC Bit Mask** – Hexidecimal mask for source or destination MAC address.
- **VID** – VLAN ID. (Range: 1-4093)
- **VID Bit Mask** – VLAN bitmask. (Range: 1-4093)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)

  A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bit Mask** – Protocol bitmask. (Range: 600-fff hex.)
- **Packet Format** – This attribute includes the following packet types:
  - **Any** – Any Ethernet packet type.
  - **Untagged-eth2** – Untagged Ethernet II packets.
  - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
  - **Tagged-eth2** – Tagged Ethernet II packets.
  - **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Web – Specify the action (i.e., Permit or Deny). Specify the source and/or destination addresses. Select the address type (Any, Host, or MAC). If you select “Host,” enter a specific address (e.g., 11-22-33-44-55-66). If you select “MAC,” enter a base address and a hexidecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.



MAC ACL

Name: bob

Action	Source MAC Address	Source Bitmask	Destination MAC Address	Destination Bitmask	VID	VID Bitmask	Ethernet Type	Ethernet Type Bitmask	Packet Format	Remove
Permit	Any	Any	00-e0-29-94-34-de	ff-ff-ff-ff-ff-ff	Any	Any	2048	65535	Any	Remove

Action	Permit
Source Address Type	Any
Source MAC Address	00-00-00-00-00-00
Source Bitmask	00-00-00-00-00-00
Destination Address Type	Any
Destination MAC Address	00-00-00-00-00-00
Destination Bitmask	00-00-00-00-00-00
VID	
VID Bitmask	
Ethernet Type	
Ethernet Type Bitmask	
Packet Format	Any

Figure 7-4 ACL Configuration - MAC

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
 ethertype 0800                                                    26-13
Console(config-mac-acl)#
```

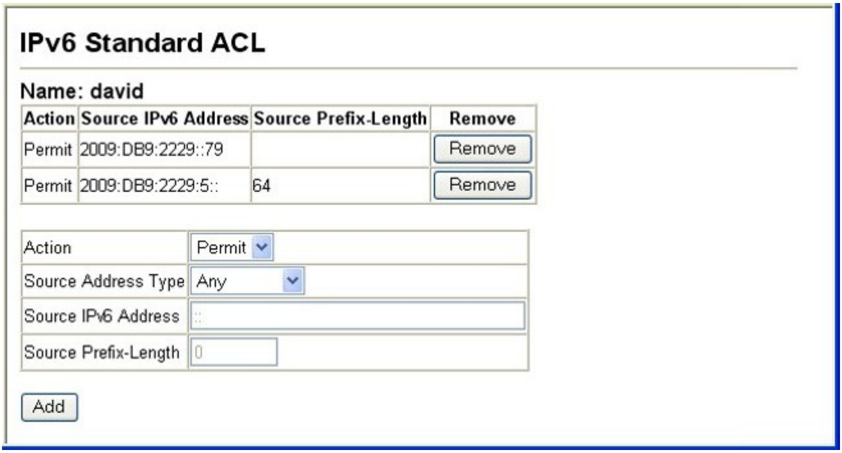
Configuring a Standard IPv6 ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Source Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IPv6-prefix” to specify a range of addresses. (Options: Any, Host, IPv6-prefix; Default: Any)
- **Source IPv6 Address** – The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- **Source Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any, Host, or IPv6-prefix). If you select “Host,” enter a specific address. If you select “IPv6-prefix,” enter a subnet address and the prefix length. Then click Add.



IPv6 Standard ACL

Name: david

Action	Source IPv6 Address	Source Prefix-Length	Remove
Permit	2009:DB9:2229::79		Remove
Permit	2009:DB9:2229:5::	64	Remove

Action	Permit
Source Address Type	Any
Source IPv6 Address	::
Source Prefix-Length	0

Figure 7-5 ACL Configuration - Standard IPv6

CLI – This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79        26-8
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

Configuring an Extended IPv6 ACL

Command Attributes

- **Action** – An ACL can contain any combination of permit or deny rules.
- **Destination Address Type** – Specifies the destination IP address. Use “Any” to include all possible addresses, or “IPv6-prefix” to specify a range of addresses. (Options: Any, IPv6-prefix; Default: Any)
- **Destination IP Address** – The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 64 bits of the destination address.)

- **Destination Prefix-Length** – A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).
- **Next Header** – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

  Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, and includes these commonly used headers:

0 :	Hop-by-Hop Options	(RFC 2460)
6 :	TCP Upper-layer Header	(RFC 1700)
17:	UDP Upper-layer Header	(RFC 1700)
43:	Routing	(RFC 2460)
44:	Fragment	(RFC 2460)
51:	Authentication	(RFC 2402)
50:	Encapsulating Security Payload	(RFC 2406)
60:	Destination Options	(RFC 2460)

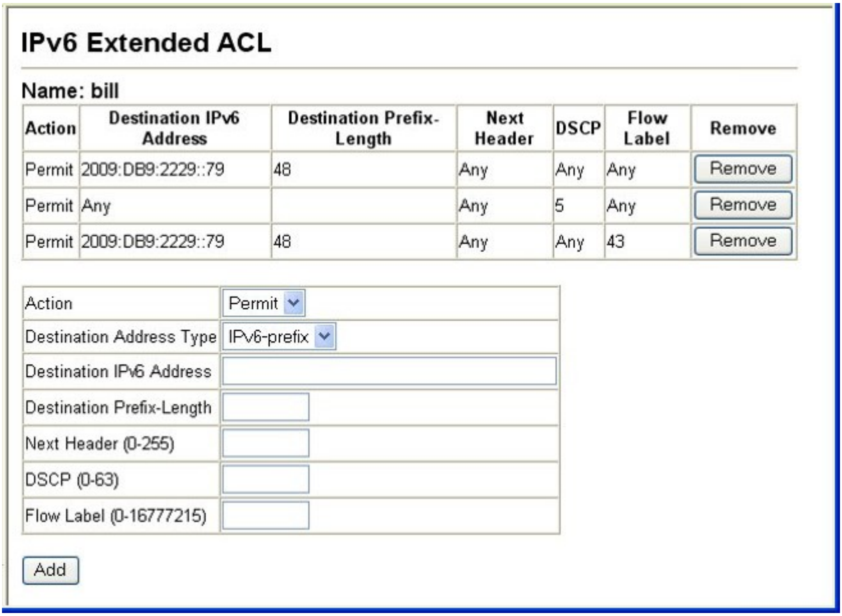
- **DSCP** – DSCP priority level. (Range: 0-63)
- **Flow Label** – A label for packets belonging to a particular traffic “flow” for which the sender requests special handling by IPv6 routers, such as non-default quality of service or “real-time” service (see RFC 2460). (Range: 0-16777215)

  A flow label is assigned to a flow by the flow's source node. New flow labels must be chosen pseudo-randomly and uniformly from the range 1 to FFFFF hexadecimal. The purpose of the random allocation is to make any set of bits within the Flow Label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

  A flow identifies a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option. A flow is uniquely identified by the combination of a source address and a non-zero flow label. Packets that do not belong to a flow carry a flow label of zero.

  Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

Web – Specify the action (i.e., Permit or Deny). Select the address type (Any or IPv6-prefix). If you select “IPv6-prefix,” enter a subnet address and prefix length. Set any other required criteria, such as next header, DSCP, or flow label. Then click Add.



IPv6 Extended ACL

Name: bill

Action	Destination IPv6 Address	Destination Prefix-Length	Next Header	DSCP	Flow Label	Remove
Permit	2009:DB9:2229::79	48	Any	Any	Any	Remove
Permit	Any		Any	5	Any	Remove
Permit	2009:DB9:2229::79	48	Any	Any	43	Remove

Action	Permit
Destination Address Type	IPv6-prefix
Destination IPv6 Address	
Destination Prefix-Length	
Next Header (0-255)	
DSCP (0-63)	
Flow Label (0-16777215)	

Figure 7-6 ACL Configuration - Extended IPv6

CLI – This example adds three rules:

1. Accepts any incoming packets for the destination 2009:DB9:2229::79/48.
2. Allows packets to any destination address when the DSCP value is 5.
3. Allows any packets sent to the destination 2009:DB9:2229::79/48 when the flow label is 43.

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48               26-9
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 flow-label 43
Console(config-ext-ipv6-acl)#
```

Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), you should bind them to the ports that need to filter traffic. You can only bind a port to one ACL for each basic type – IPv4 ingress, MAC ingress, and IPv6 ingress.

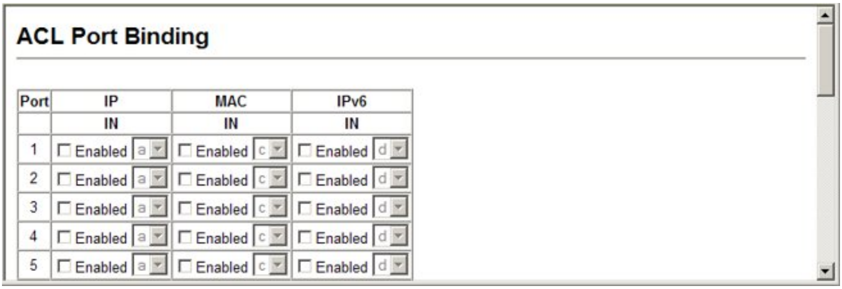
Command Usage

- This switch supports ACLs for ingress filtering only.

Command Attributes

- **Port** – Fixed port, SFP module, or XFP module. (Range: 1-26/50)
- **IP** – Specifies the IPv4 ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IPv6** – Specifies the IPv6 ACL to bind to a port.
- **IN** – ACL for ingress packets.
- *ACL Name* – Name of the ACL.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port you want to bind to an ACL for ingress traffic, select the required ACL from the drop-down list, then click Apply.



ACL Port Binding

Port	IP	MAC	IPv6
	IN	IN	IN
1	□ Enabled a	□ Enabled c	□ Enabled d
2	□ Enabled a	□ Enabled c	□ Enabled d
3	□ Enabled a	□ Enabled c	□ Enabled d
4	□ Enabled a	□ Enabled c	□ Enabled d
5	□ Enabled a	□ Enabled c	□ Enabled d

Figure 7-7 ACL Port Binding

CLI – This examples assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1                                27-1
Console(config-if)#ip access-group tom in                             26-6
Console(config-if)#mac access-group jerry in                         26-15
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group tom in
Console(config-if)#
```

Chapter 8: Port Configuration

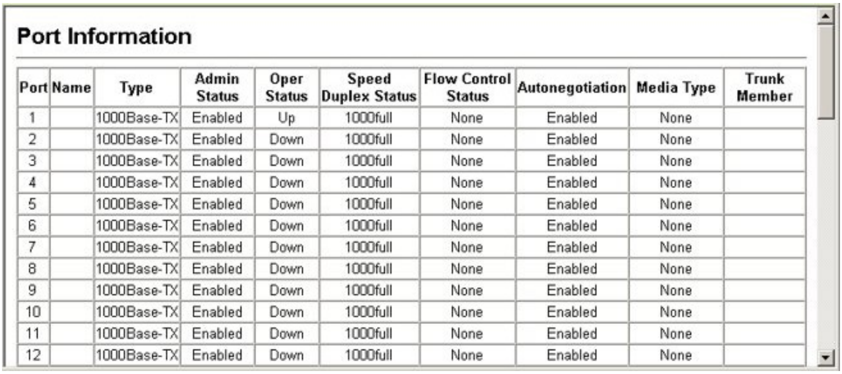
Displaying Connection Status

You can use the Port Information or Trunk Information pages to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type. (1000BASE-T, SFP, or 10G)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Flow Control Status** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Media Type**[4] – Shows the forced/preferred port type to use for combination ports 21-24 (IC40240-10G) or 45-48 (IC40480-10G). (Copper-Forced, SFP-Forced, SFP-Preferred-Auto)
- **Trunk Member**[4] – Shows if port is a trunk member.
- **Creation**[5] – Shows if a trunk is manually configured or dynamically set via LACP.

Web – Click Port, Port Information or Trunk Information.



Port Information

Port	Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1		1000Base-TX	Enabled	Up	1000full	None	Enabled	None	
2		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
3		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
4		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
5		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
6		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
7		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
8		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
9		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
10		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
11		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	
12		1000Base-TX	Enabled	Down	1000full	None	Enabled	None	

Figure 8-1 Port - Port Information

[4] Port Information only.
[5] Trunk Information only.

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (1000BASE-T, SFP, or 10G)
- **MAC address** – The physical layer address for this port. (To access this item on the web, see “Setting the Switch’s IP Address (IP Version 4)” on page 4-5.)

Configuration:

- **Name** – Interface label.
- **Port admin** – Shows if the interface is enabled or disabled (i.e., up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see “Configuring Interface Connections” on page 3-48.) The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation
  - **1000full** - Supports 1000 Mbps full-duplex operation
  - **10Gfull** - Supports 10 Gbps full-duplex operation
  - **Sym** - Transmits and receives pause frames for flow control
  - **FC** - Supports flow control
- **Broadcast storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast storm limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port security** – Shows if port security is enabled or disabled.
- **Max MAC count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 1024 addresses)
- **Port security action** – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)
- **Media type** – Shows the forced/preferred port type to use for combination ports 21-24 (IC40240-10G) or 45-48 (IC40480-10G). (copper forced, SFP forced, SFP preferred auto)

Current status:

- **Link status** – Indicates if the link is up or down.
- **Port operation status** – Provides detailed information on port state. (Displayed only when the link is up.).
- **Operation speed-duplex** – Shows the current speed and duplex mode.
- **Flow control type** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or none)

CLI – This example shows the connection status for Port 5.

```
Console#show interfaces status ethernet 1/5                                   27-9
Information of Eth 1/13
 Basic information:
  Port type:                 1000T
  Mac address:                00-30-F1-D4-73-A5
 Configuration:
  Name:
  Port admin:                Up
  Speed-duplex:              Auto
  Capabilities:                 10half, 10full, 100half, 100full, 1000full
  Broadcast storm:           Enabled
  Broadcast storm limit:    500 packets/second
  Flow control:              Disabled
  LACP:                      Disabled
  Port security:             Disabled
  Max MAC count:            0
  Port security action:      None
  Media type:                None
 Current status:
  Link status:               Down
  Operation speed-duplex:   1000full
  Flow control type:         None
Console#
```

Configuring Interface Connections

You can use the Port Configuration or Trunk Configuration page to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed and duplex mode, and flow control.

Command Attributes

- **Name** – Allows you to label an interface. (Range: 1-64 characters)
- **Admin** – Allows you to manually disable an interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Allows you to manually set the port speed and duplex mode (i.e., with auto-negotiation disabled).

  Note: The 1000BASE-T standard does not support forced mode. Always use auto-negotiation to establish a connection over any 1000BASE-T port or trunk.
- **Flow Control** – Allows automatic or manual selection of flow control.
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, you need to specify the capabilities to be advertised. When auto-negotiation is disabled, you can force the settings for speed, duplex mode, and flow control. The following capabilities are supported.
  - **10half** - Supports 10 Mbps half-duplex operation
  - **10full** - Supports 10 Mbps full-duplex operation
  - **100half** - Supports 100 Mbps half-duplex operation
  - **100full** - Supports 100 Mbps full-duplex operation

- **1000full** - Supports 1 Gbps full-duplex operation
- **10Gfull** - Supports 10 Gbps full-duplex operation
- **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current switch chip only supports symmetric pause frames.*)
- **FC** - Supports flow control
  Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

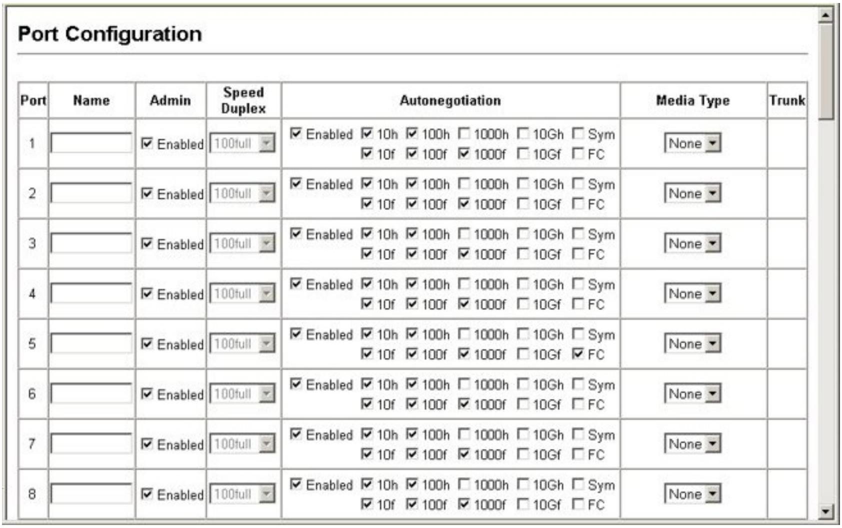
(Default: Autonegotiation enabled; Advertised capabilities for
1000BASE-T – 10half, 10full, 100half, 100full, 1000full;
1000BASE-SX/LX/LH – 1000full;

10GBASE-SR/LR/ER – 10Gfull)

- **Media Type** – Shows the forced/preferred port type to use for the combination ports. (IC40240-10G: Ports 21-24; IC40480-10G: Ports 45-48)
  - **Copper-Forced** - Always uses the built-in RJ-45 port.
  - **SFP-Forced** - Always uses the SFP port (even if module is not installed).
  - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see “Creating Trunk Groups” on page 8-6.

Note: Auto-negotiation must be disabled before you can configure or force the interface to use the Speed/Duplex Mode or Flow Control options.

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.



Port Configuration

Port	Name	Admin	Speed Duplex	Autonegotiation	Media Type	Trunk
1		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	
2		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	
3		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	
4		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	
5		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf ☑ FC	None	
6		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	
7		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	
8		☑ Enabled	100full	☑ Enabled ☑ 10h ☑ 100h □ 1000h □ 10Gh □ Sym ☑ 10f ☑ 100f ☑ 1000f □ 10Gf □ FC	None	

Figure 8-2 Port - Port Configuration

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13                                  27-1
Console(config-if)#description RD SW#13                                  27-2
Console(config-if)#shutdown                                              27-7
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation                                        27-4
Console(config-if)#speed-duplex 100half                                  27-3
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half                                  27-4
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#exit
Console(config)#interface ethernet 1/21
Console(config-if)#media-type copper-forced                              27-6
Console(config-if)#
```

Creating Trunk Groups

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices (i.e., single switch or a stack). You can create up to 32 trunks.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

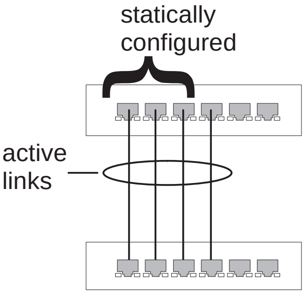
Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 32 trunks on a switch or stack, with up to eight Gigabit ports per trunk or up to four 10Gbps ports per trunk. Note that because the stack functions conceptually as a single system, you can include ports from different units in the same trunk. For example, you could connect ports spread across several units that belong VLAN 2 into a common trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (i.e., speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

Statically Configuring a Trunk

Command Usage

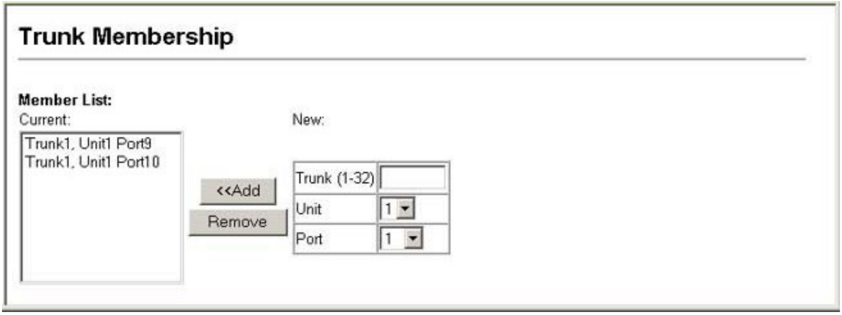
- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer’s implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk via the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk via the configuration interface.



Command Attributes

- **Member List** (Current) – Shows configured trunks (Trunk ID, Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Trunk** – Trunk identifier. (Range: 1-32)
  - **Unit** – Stack unit. (Range: 1-8)
  - **Port** – Port identifier. (Range: 1-25/49)

Web – Click Port, Trunk Membership. Enter a trunk ID of 1-32 in the Trunk field, select any of the switch ports from the scroll-down port list, and click Add. After you have completed adding ports to the member list, click Apply.



Trunk Membership

Member List:

Current:

Trunk1, Unit1 Port9
Trunk1, Unit1 Port10

New:

Trunk (1-32)	
Unit	1
Port	1

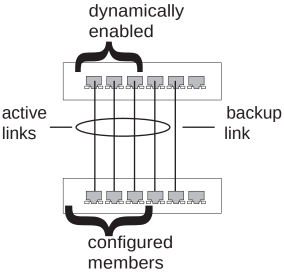
Figure 8-3 Static Trunk Configuration

CLI – This example creates trunk 1 with ports 9 and 10. Just connect these ports to two static trunk ports on another switch to form a trunk.

```
Console(config)#interface port-channel 1                             27-1
Console(config-if)#exit
Console(config)#interface ethernet 1/9                               27-1
Console(config-if)#channel-group 1                                   28-2
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1                        27-9
Information of Trunk 1
 Basic information:
  Port type:              1000T
  Mac address:            00-30-F1-D4-73-A2
 Configuration:
  Name:
  Port admin:             Up
  Speed-duplex:           Auto
  Capabilities:           10half, 10full, 100half, 100full, 1000full
  Flow control:           Disabled
  Port security:          Disabled
  Max MAC count:          0
 Current status:
  Created by:             User
  Link status:            Up
  Port operation status:  Up
  Operation speed-duplex: 1000full
  Flow control type:      None
  Member Ports: Eth1/9, Eth1/10,
Console#
```

Enabling LACP on Selected Ports

Command Usage

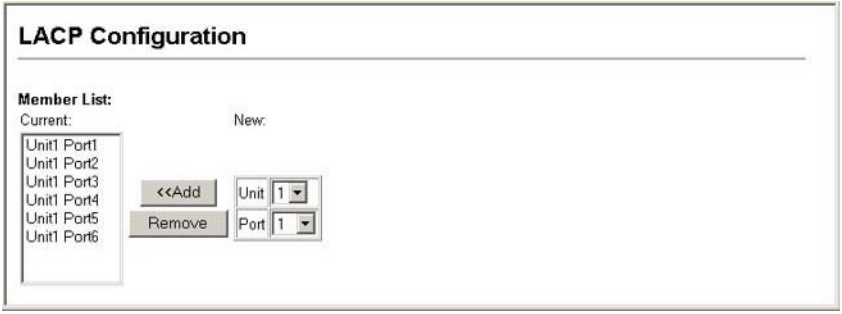


- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- Trunks dynamically established through LACP will also be shown in the Member List on the Trunk Membership menu (see page 8-7).

Command Attributes

- **Member List** (Current) – Shows configured trunks (Unit, Port).
- **New** – Includes entry fields for creating new trunks.
  - **Unit** – Stack unit. (Range: 1-8)
  - **Port** – Port identifier. (Range: 1-25/49)

Web – Click Port, LACP, Configuration. Select any of the switch ports from the scroll-down port list and click Add. After you have completed adding ports to the member list, click Apply.



LACP Configuration

Member List:

Current:

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port5
Unit1 Port6

New:

Unit 1

Port 1

Figure 8-4 LACP Trunk Configuration

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```
Console(config)#interface ethernet 1/1                                   27-1
Console(config-if)#lacp                                                  28-3
Console(config-if)#exit
:
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1                            27-9
Information of Trunk 1
 Basic information:
  Port type:                1000T
  Mac address:              00-30-F1-D4-73-A2
 Configuration:
  Port admin:               Up
  Speed-duplex:             Auto
  Capabilities:             10half, 10full, 100half, 100full, 1000full
  Flow control:             Disabled
  Port security:            Disabled
  Max MAC count:            0
 Current status:
  Created by:               LACP
  Link status:              Up
  Port operation status:    Up
  Operation speed-duplex:   1000full
  Flow control type:        None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,
Console#
```

Configuring LACP Parameters

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the “port channel” Admin Key is set (page 4-142), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

  Note – If the port channel admin key (lacp admin key, page 28-6) is not set (through the CLI) when a channel group is formed (i.e., it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 28-5).

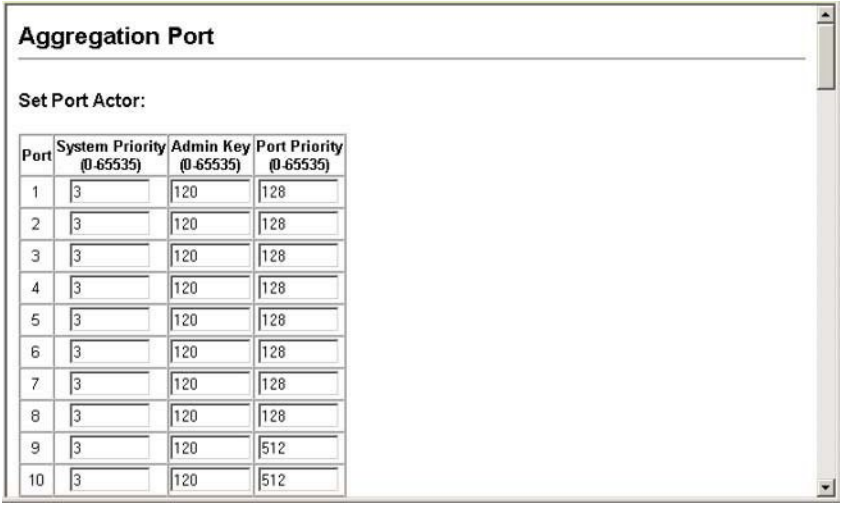
Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; i.e., the ports on this switch.

- **Port** – Port number. (Range: 1-25/49)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
  - Ports must be configured with the same system priority to join the same LAG.
  - System priority is combined with the switch’s MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; i.e., the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. You can optionally configure these settings for the Port Partner. (Be aware that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After you have completed setting the port LACP parameters, click Apply.



Aggregation Port

Set Port Actor:

Port	System Priority (0-65535)	Admin Key (0-65535)	Port Priority (0-65535)
1	3	120	128
2	3	120	128
3	3	120	128
4	3	120	128
5	3	120	128
6	3	120	128
7	3	120	128
8	3	120	128
9	3	120	512
10	3	120	512

Figure 8-5 LACP - Aggregation Port

CLI – The following example configures LACP parameters for ports 1-10. Ports 1-8 are used as active members of the LAG, ports 9 and 10 are set to backup mode.

```
Console(config)#interface ethernet 1/1                               27-1
Console(config-if)#lacp actor system-priority 3                      28-4
Console(config-if)#lacp actor admin-key 120                          28-5
Console(config-if)#lacp actor port-priority 128                      28-6
Console(config-if)#exit
:
Console(config)#interface ethernet 1/10
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid                                              28-7
Channel Group     System Priority     System MAC Address
------------------------------------------------------------------------
            1                   3      00-00-E9-31-31-31
            2               32768      00-00-E9-31-31-31
            3               32768      00-00-E9-31-31-31
:
Console#show lacp 1 internal                                         28-7
Port channel: 1
------------------------------------------------------------------------
Oper Key:   120
Admin Key: 0
Eth 1/ 1
------------------------------------------------------------------------
  LACPDUs Internal:       30 sec
  LACP System Priority: 3
  LACP Port Priority:     128
  Admin Key:              120
  Oper Key:               120
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:                distributing, collecting, synchronization,
                        aggregation, long timeout, LACP-activity
:
```

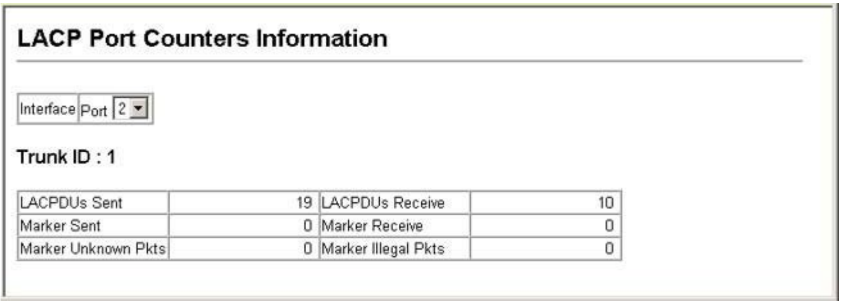
Displaying LACP Port Counters

You can display statistics for LACP protocol messages.

Table 8-1 LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received by this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker I legal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Web – Click Port, LACP, Port Counters Information. Select a member port to display the corresponding information.



LACP Port Counters Information

Interface Port 2

Trunk ID : 1

LACPDUs Sent	19	LACPDUs Receive	10
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

Figure 8-6 LACP - Port Counters Information

CLI – The following example displays LACP counters for port channel 1.

```
Console#show lacp 1 counters                                         28-7
Port channel: 1
-------------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------------
  LACPDUs Sent:           19
  LACPDUs Receive:        10
  Marker Sent:            0
  Marker Receive:         0
  LACPDUs Unknown Pkts: 0
  LACPDUs Illegal Pkts: 0
:
```

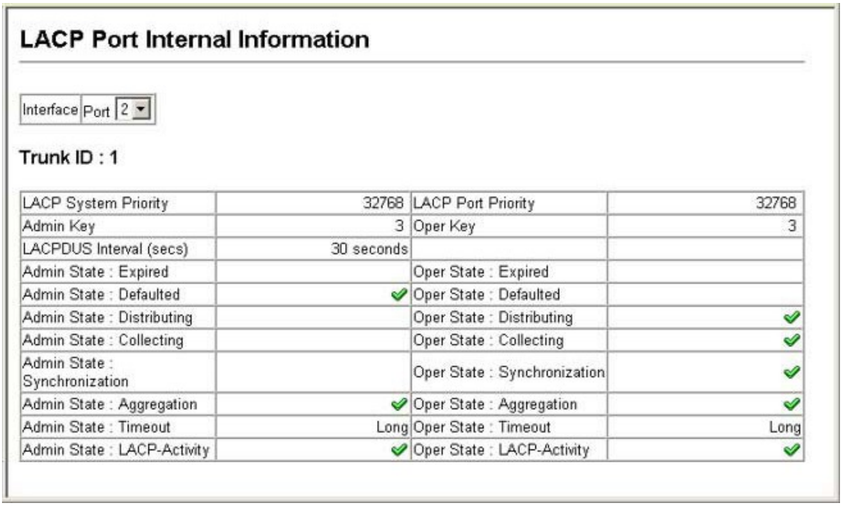
Displaying LACP Settings and Status for the Local Side

You can display configuration settings and the operational state for the local side of an link aggregation.

Table 8-2 LACP Internal Configuration Information

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.



LACP Port Internal Information

Interface Port 2

Trunk ID : 1

LACP System Priority	32768	LACP Port Priority	32768
Admin Key	3	Oper Key	3
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	✓
Admin State : Collecting		Oper State : Collecting	✓
Admin State : Synchronization		Oper State : Synchronization	✓
Admin State : Aggregation	✓	Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity	✓	Oper State : LACP-Activity	✓

Figure 8-7 LACP - Port Internal Information

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```
Console#show lacp 1 internal                                        28-7
Port channel: 1
-----------------------------------------------------------------------
Oper Key:   3
Admin Key: 0
Eth 1/ 2
-----------------------------------------------------------------------
  LACPDUs Internal:       30 sec
  LACP System Priority: 32768
  LACP Port Priority:     32768
  Admin Key:             3
  Oper Key:              3
  Admin State: defaulted, aggregation, long timeout, LACP-activity
  Oper State:               distributing, collecting, synchronization,
                         aggregation, long timeout, LACP-activity
:
```

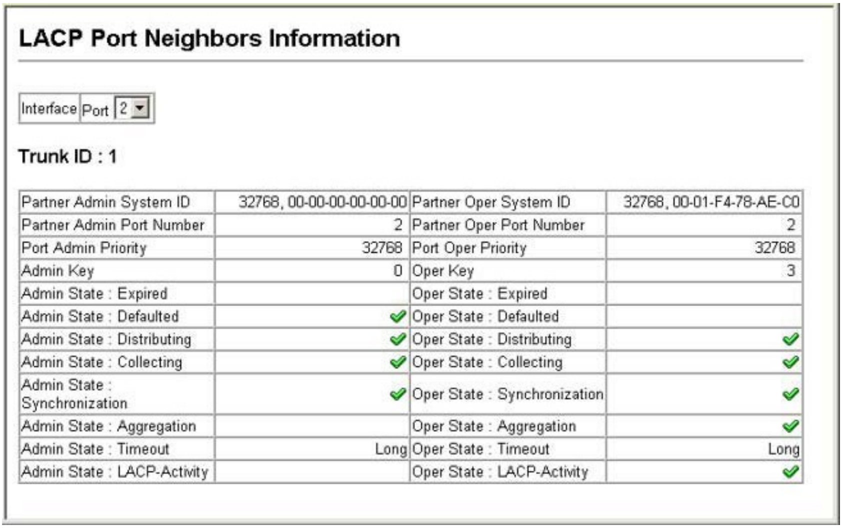
Displaying LACP Settings and Status for the Remote Side

You can display configuration settings and the operational state for the remote side of an link aggregation.

Table 8-3 LACP Neighbor Configuration Information

Field	Description
Partner Admin System ID	LAG partner’s system ID assigned by the user.
Partner Oper System ID	LAG partner’s system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port’s protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner’s state parameters. (See preceding table.)
Oper State	Operational values of the partner’s state parameters. (See preceding table.)

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.



LACP Port Neighbors Information

Interface Port 2

Trunk ID : 1

Partner Admin System ID	32768, 00-00-00-00-00-00	Partner Oper System ID	32768, 00-01-F4-78-AE-C0
Partner Admin Port Number	2	Partner Oper Port Number	2
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	3
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing	✓	Oper State : Distributing	✓
Admin State : Collecting	✓	Oper State : Collecting	✓
Admin State : Synchronization	✓	Oper State : Synchronization	✓
Admin State : Aggregation		Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✓

Figure 8-8 LACP - Port Neighbors Information

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```
Console#show lacp 1 neighbors                                         28-7
Port channel 1 neighbors
-------------------------------------------------------------------------
Eth 1/2
-------------------------------------------------------------------------
  Partner Admin System ID:   32768, 00-00-00-00-00-00
  Partner Oper System ID:      32768, 00-01-F4-78-AE-C0
  Partner Admin Port Number: 2
  Partner Oper Port Number:  2
  Port Admin Priority:       32768
  Port Oper Priority:        32768
  Admin Key:                 0
  Oper Key:                  3
  Admin State:                 defaulted, distributing, collecting,
                             synchronization, long timeout,
  Oper State:                  distributing, collecting, synchronization,
                             aggregation, long timeout, LACP-activity
:
```

Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

Command Usage

- Broadcast control does not effect IP multicast traffic.
- The resolution is 1 packet per second (pps); i.e., any setting between 500-262143 is acceptable.

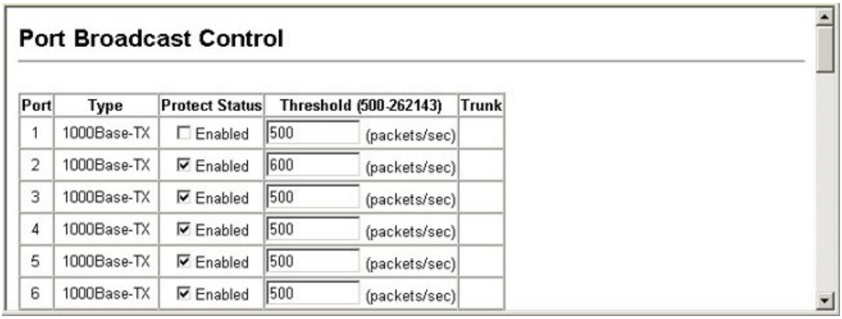
Command Attributes

- **Port**[6] – Port number.
- **Trunk**[7] – Trunk number
- **Type** – Indicates the port type. (1000BASE-T, SFP, or 10G)
- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (Options: 500-262143 packets per second; Default: 500 pps)
- **Trunk**[6] – Shows if port is a trunk member.

[6] Port Broadcast Control

[7] Trunk Broadcast Control

Web – Click Port, Port Broadcast Control or Trunk Broadcast Control. Check the Enabled box for any interface, set the threshold, and click Apply.



Port Broadcast Control

Port	Type	Protect Status	Threshold (500-262143)	Trunk
1	1000Base-TX	□ Enabled	500 (packets/sec)	
2	1000Base-TX	☑ Enabled	600 (packets/sec)	
3	1000Base-TX	☑ Enabled	500 (packets/sec)	
4	1000Base-TX	☑ Enabled	500 (packets/sec)	
5	1000Base-TX	☑ Enabled	500 (packets/sec)	
6	1000Base-TX	☑ Enabled	500 (packets/sec)	

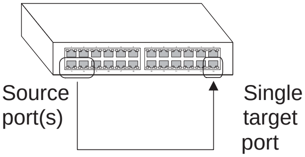
Figure 8-9 Port Broadcast Control

CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.

```
Console(config)#interface ethernet 1/1                               27-1
Console(config-if)#no switchport broadcast                           27-7
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 600              27-7
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2                     27-11
Information of Eth 1/2
 Broadcast threshold:              Enabled, 600 packets/second
 LACP status:                     Disabled
 Ingress rate limit:               Disable, 1000M bits per second
 Egress rate limit:                Disable, 1000M bits per second
 VLAN membership mode:            Hybrid
 Ingress rule:                    Disabled
 Acceptable frame type:           All frames
 Native VLAN:                     1
 Priority for untagged traffic: 0
 GVRP status:                     Disabled
 Allowed VLAN:                    1(u),
 Forbidden VLAN:
Console#
```

Configuring Port Mirroring

You can mirror traffic from any source port to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source port in a completely unobtrusive manner.



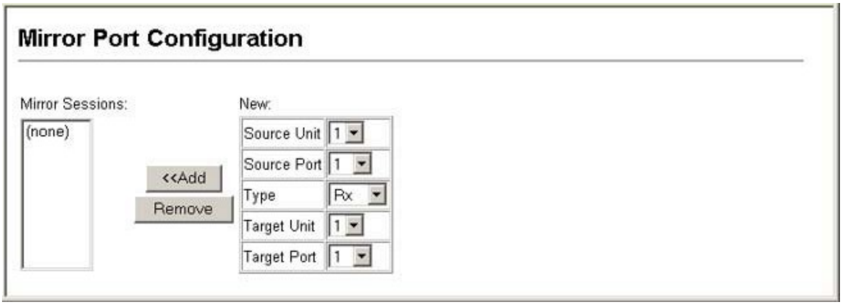
Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port when using MSTP (see “Spanning Tree Algorithm” on page 10-1).

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Unit** – The unit whose port traffic will be monitored. (Range: 1-8)
- **Source Port** – The port whose traffic will be monitored. (Range: 1-26/50)
- **Type** – Allows you to select which traffic to mirror to the target port, Rx (receive), Tx (transmit), or Both. (Default: Rx)
- **Target Unit** – The unit whose port will "duplicate" or "mirror" the traffic on the source port. (Range: 1-8)
- **Target Port** – The port that will “mirror” the traffic from the source port. (Range: 1-26/50)

Web – Click Port, Mirror Port Configuration. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.



Mirror Port Configuration

Mirror Sessions:
(none)

New:

Source Unit	1
Source Port	1
Type	Rx
Target Unit	1
Target Port	1

Figure 8-10 Mirror Port Configuration

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/10                               27-1
Console(config-if)#port monitor ethernet 1/13                         29-1
Console(config-if)#
```

Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

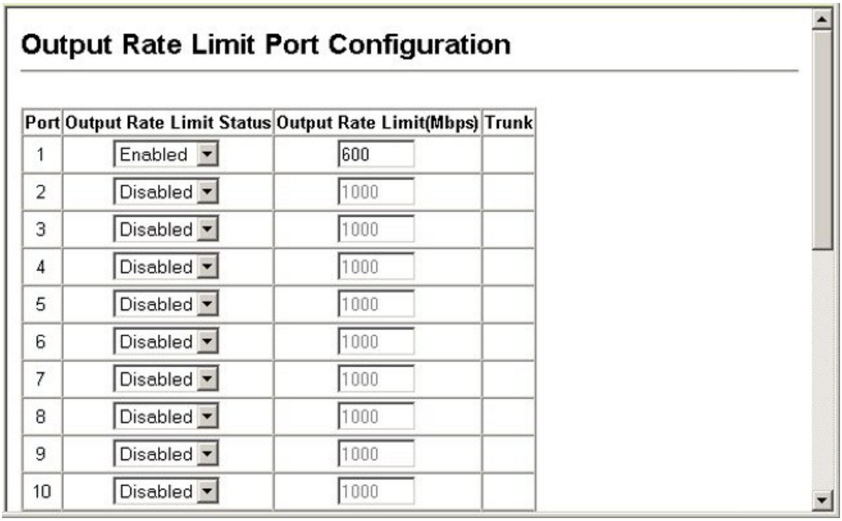
Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Command Attribute

Rate Limit – Sets the output rate limit for an interface.
Default Status – Disabled
Default Rate – Gigabit Ethernet: 1000 Mbps
Range – Gigabit Ethernet: 1 - 1000 Mbps

Note: Rate limits are not supported for the 10 Gigabit Ethernet ports.

Web - Click Port, Rate Limit, Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.



Output Rate Limit Port Configuration

Port	Output Rate Limit Status	Output Rate Limit(Mbps)	Trunk
1	Enabled	600	
2	Disabled	1000	
3	Disabled	1000	
4	Disabled	1000	
5	Disabled	1000	
6	Disabled	1000	
7	Disabled	1000	
8	Disabled	1000	
9	Disabled	1000	
10	Disabled	1000	

Figure 8-11 Rate Limit Configuration

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 600 Mbps.

```
Console(config)#interface ethernet 1/1                              27-1
Console(config-if)#rate-limit input 600                             30-1
Console(config-if)#rate-limit output 600
Console(config-if)#
```

Showing Port Statistics

You can display standard statistics on network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as HP OpenView.

Table 8-4 Port Statistics

Parameter	Description
Interface Statistics	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

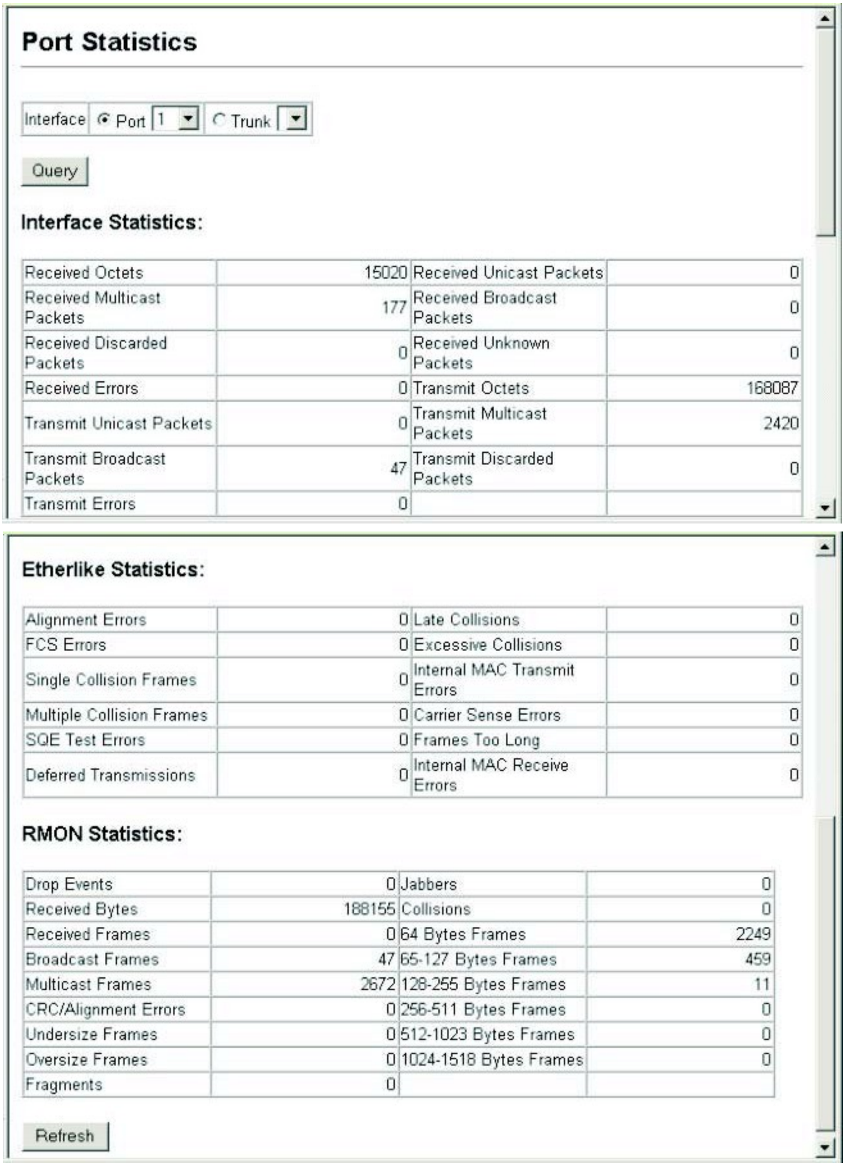
Table 8-4 Port Statistics (Continued)

Parameter	Description
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
Etherlike Statistics	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
RMON Statistics	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.

Table 8-4 Port Statistics (Continued)

Parameter	Description
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Port, Port Statistics. Select the required interface, and click Query. You can also use the Refresh button at the bottom of the page to update the screen.



Port Statistics

Interface ● Port 1 ○ Trunk

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Figure 8-12 Port Statistics

CLI – This example shows statistics for port 12.

```
Console#show interfaces counters ethernet 1/12                             27-10
Ethernet 1/12
 Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
 Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
 Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
 RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

Chapter 9: Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

Setting Static Addresses

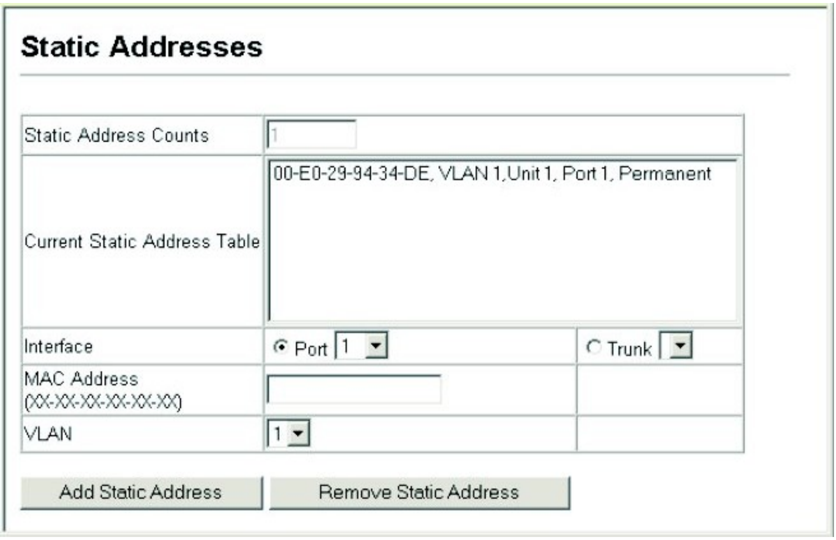
A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Static Address Counts**[8] – The number of manually configured addresses.
- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4093).

[8] Web Only.

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.



Static Addresses

Static Address Counts	1	
Current Static Address Table	00-E0-29-94-34-DE, VLAN 1,Unit 1, Port 1, Permanent	
Interface	● Port 1	○ Trunk
MAC Address (XX-XX-XX-XX-XX-XX)		
VLAN	1	

Figure 9-1 Static Addresses

CLI – This example adds an address to the static address table, but sets it to be deleted when the switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
 ethernet 1/1 vlan 1 delete-on-reset                                 31-1
Console(config)#
```

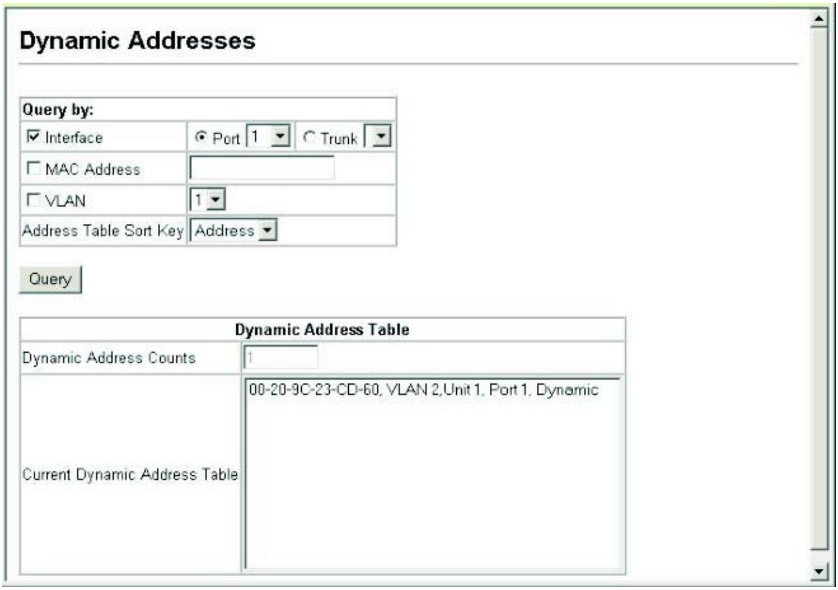
Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.
- **VLAN** – ID of configured VLAN (1-4093).
- **Address Table Sort Key** – You can sort the information displayed based on MAC address, VLAN or interface (port or trunk).
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

Web – Click Address Table, Dynamic Addresses. Specify the search type (i.e., mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.



Dynamic Addresses

Query by:	
☑ Interface	● Port 1 ○ Trunk
□ MAC Address	
□ VLAN	1
Address Table Sort Key	Address

Query

Dynamic Address Table	
Dynamic Address Counts	1
Current Dynamic Address Table	00-20-9C-23-CD-60, VLAN 2,Unit 1, Port 1, Dynamic

Figure 9-2 Dynamic Addresses

CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1              31-3
 Interface Mac Address          Vlan Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-E0-29-94-34-DE    1 Permanent
  Eth 1/ 1 00-20-9C-23-CD-60    2 Learned
Console#
```

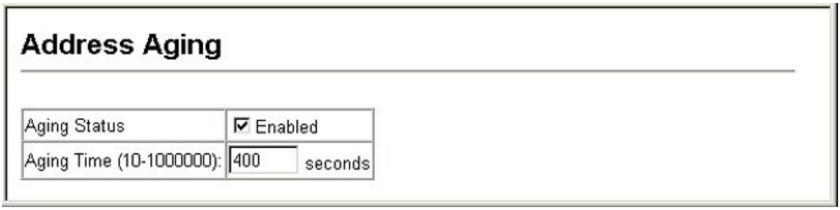
Changing the Aging Time

You can set the aging time for entries in the dynamic address table.

Command Attributes

- **Aging Status** – Enables/disables the aging function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.



Address Aging

Aging Status	☑ Enabled
Aging Time (10-1000000):	400 seconds

Figure 9-3 Address Aging

CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400                    31-4
Console(config)#
```

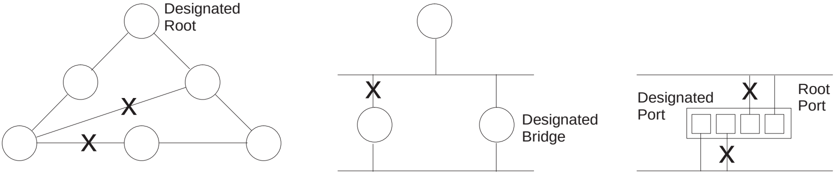
Chapter 10: Spanning Tree Algorithm

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

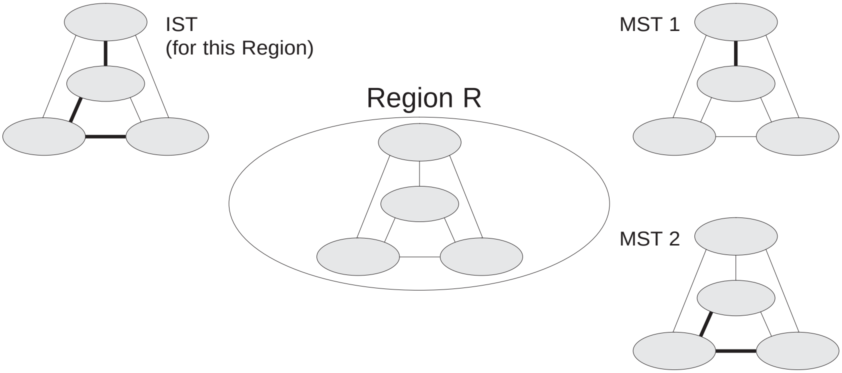
STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



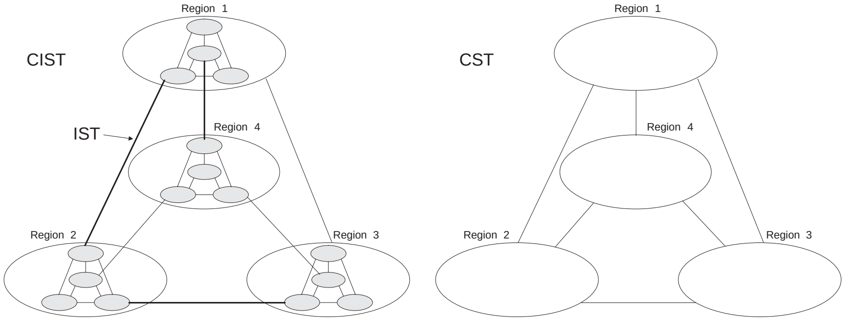
Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves must faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.



An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including the Region Name, Revision Level and Configuration Digest – see “Configuring Multiple Spanning Trees” on page 16). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.



MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

Displaying Global Settings

You can display a summary of the current bridge STA information that applies to the entire switch using the STA Information screen.

Field Attributes

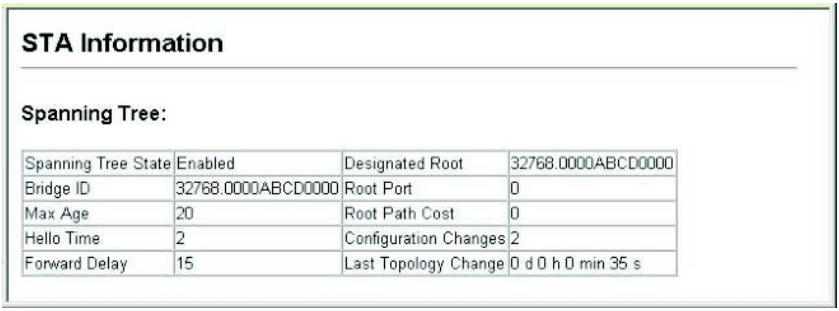
- **Spanning Tree State** – Shows if the switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree mode is set to MSTP (page 10-6), and MAC address (where the address is taken from the switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
  - **Root Port** – The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.
  - **Root Path Cost** – The path cost from the root port on this switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D)
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)

- **Instance** – Instance identifier of this spanning tree. (This is always 0 for the CIST.)
- **VLANs configuration** – VLANs assigned to the CIST.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)
- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Max hops** – The max number of hop counts for the MST region.
- **Remaining hops** – The remaining number of hop counts for the MST instance.
- **Transmission limit** – The minimum interval between the transmission of consecutive RSTP/MSTP BPDUs.
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.



STA Information

Spanning Tree:

Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

Figure 10-1 STA Information

CLI – This command displays global STA settings, followed by settings for each port.

```
Console#show spanning-tree                                             33-18
Spanning-tree information
-------------------------------------------------------------------
 Spanning Tree Mode:                    MSTP
 Spanning Tree Enabled/Disabled:        Enabled
 Instance:                              0
 VLANs Configuration:                   1-4093
 Priority:                              32768
 Bridge Hello Time (sec.):              2
 Bridge Max Age (sec.):                 20
 Bridge Forward Delay (sec.):           15
 Root Hello Time (sec.):                2
 Root Max Age (sec.):                   20
 Root Forward Delay (sec.):             15
 Max  Hops:                             20
 Remaining Hops:                        20
 Designated Root:                        32768.0.0001ECF8D8C6
 Current Root Port:                     1
 Current Root Cost:                     100000
 Number of Topology Changes:            1
 Last Topology Change Time (sec.): 1521
 Transmission Limit:                    3
 Path Cost Method:                      Long

-------------------------------------------------------------------
Eth    1/ 1 information
-------------------------------------------------------------------
 Admin Status:                 Enabled
 Role:                         root
 State:                        forwarding
 External Admin Path Cost: 0
 Internal Admin Path Cost: 0
 External Oper Path Cost:  100000
 Internal Oper Path Cost:  100000
 Priority:                     128
 Designated Cost:              0
 Designated Port:              128.15
 Designated Root:               32768.0.0001ECF8D8C6
 Designated Bridge:             32768.0.0001ECF8D8C6
 Fast Forwarding:              Disabled
 Forward Transitions:          1
 Admin Edge Port:              Disabled
 Oper Edge Port:               Disabled
 Admin Link Type:              auto
 Oper Link Type:                Point-to-point
 Spanning   Tree   Status:                    Enabled
.
.
.
```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

Configuring Global Settings

Global settings apply to the entire switch.

Command Usage

- Spanning Tree Protocol[9]

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol[9]

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on this switch. (Default: Enabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on this switch:
  - **STP**: Spanning Tree Protocol (IEEE 802.1D); i.e., when this option is selected, the switch will use RSTP set to STP forced compatibility mode).
  - **RSTP**: Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
  - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC

[9] STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

address will then become the root device. (Note that lower numeric values indicate higher priority.)

  - Default: 32768
  - Range: 0-61440, in steps of 4096
  - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
  - Default: 2
  - Minimum: 1
  - Maximum: The lower of 10 or [(Max. Message Age / 2) -1]
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
  - Default: 20
  - Minimum: The higher of 6 or [2 x (Hello Time + 1)].
  - Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - Default: 15
  - Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  - Maximum: 30

Configuration Settings for RSTP

The following attributes apply to both RSTP and MSTP:

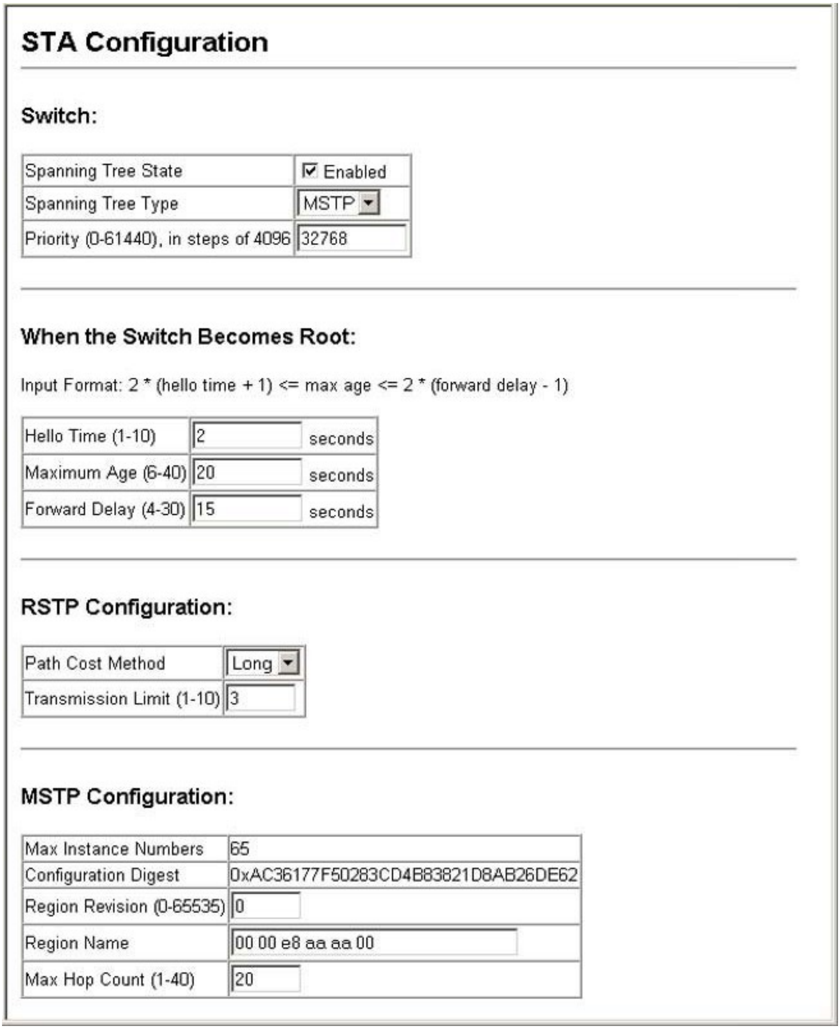
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
  - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
  - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Configuration Settings for MSTP

- **Max Instance Numbers** – The maximum number of MSTP instances to which this switch can be assigned. (Default: 33)
- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- **Region Revision**[10] – The revision for this MSTI. (Range: 0-65535; Default: 0)
- **Region Name**[10] – The name for this MSTI. (Maximum length: 32 characters)
- **Max Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

[10] The MST name and revision number are both required to uniquely identify an MST region.

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, and click Apply.



STA Configuration

Switch:

Spanning Tree State	☑ Enabled
Spanning Tree Type	MSTP
Priority (0-61440), in steps of 4096	32768

When the Switch Becomes Root:

Input Format: 2 * (hello time + 1) <= max age <= 2 * (forward delay - 1)

Hello Time (1-10)	2	seconds
Maximum Age (6-40)	20	seconds
Forward Delay (4-30)	15	seconds

RSTP Configuration:

Path Cost Method	Long
Transmission Limit (1-10)	3

MSTP Configuration:

Max Instance Numbers	65
Configuration Digest	0xAC36177F50283CD4B83821D8AB26DE62
Region Revision (0-65535)	0
Region Name	00 00 e8 aa aa 00
Max Hop Count (1-40)	20

Figure 10-2 STA Global Configuration

CLI – This example enables Spanning Tree Protocol, sets the mode to MST, and then configures the STA and MSTP parameters.

```
Console(config)#spanning-tree                                           33-2
Console(config)#spanning-tree mode mstp                                 33-2
Console(config)#spanning-tree priority 40000                            33-6
Console(config)#spanning-tree hello-time 5                              33-4
Console(config)#spanning-tree max-age 38                                33-5
Console(config)#spanning-tree forward-time 20                           33-4
Console(config)#spanning-tree pathcost method long                      33-6
Console(config)#spanning-tree transmission-limit 4                      33-7
Console(config)#spanning-tree mst-configuration                         33-7
Console(config-mstp)#revision 1                                        33-10
Console(config-mstp)#name R&D                                           33-9
Console(config-mstp)#max-hops 30                                       33-11
Console(config-mstp)#
```

Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

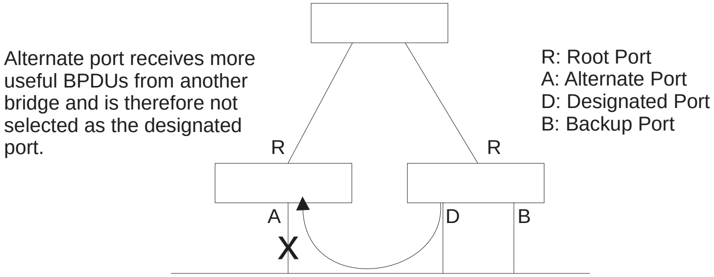
Field Attributes

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.

  The rules defining port status are:

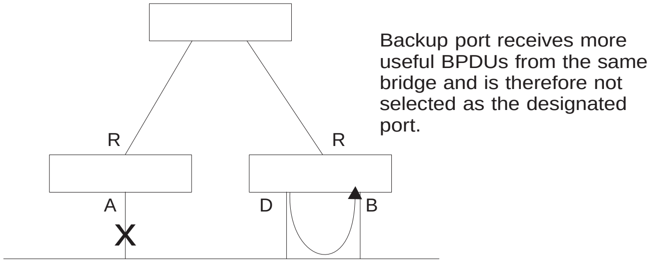
  - A port on a network segment with no other STA compliant bridging device is always forwarding.
  - If two ports of a switch are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
  - All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.

- **Designated Port** – The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** – The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Oper Link Type** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 10-13.
- **Oper Edge Port** – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 10-13 (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., **root** port), connecting a LAN through the bridge to the root bridge (i.e., **designated** port), or is the MSTI regional root (i.e., **master** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., **disabled** port) if a port has no role within the spanning tree.



Alternate port receives more useful BPDUs from another bridge and is therefore not selected as the designated port.

R: Root Port
A: Alternate Port
D: Designated Port
B: Backup Port



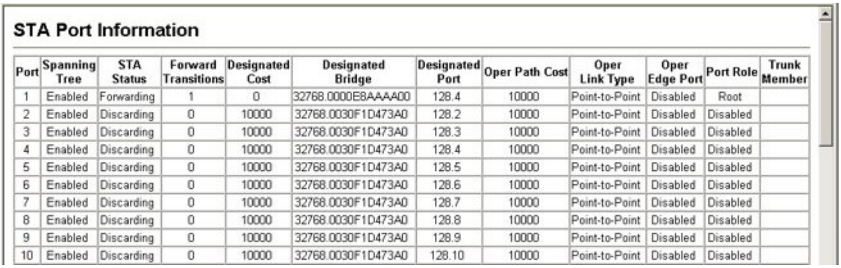
Backup port receives more useful BPDUs from the same bridge and is therefore not selected as the designated port.

- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- **External path cost** – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Internal path cost** – The path cost for the MST. See the preceding item.
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.
- **Designated root** – The priority and MAC address of the device in the Spanning Tree that this switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA, Port Information or STA Trunk Information.



STA Port Information

Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	1	0	32768.0000E8AAAA00	128.4	10000	Point-to-Point	Disabled	Root	
2	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.2	10000	Point-to-Point	Disabled	Disabled	
3	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.4	10000	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.5	10000	Point-to-Point	Disabled	Disabled	
6	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.6	10000	Point-to-Point	Disabled	Disabled	
7	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.7	10000	Point-to-Point	Disabled	Disabled	
8	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.8	10000	Point-to-Point	Disabled	Disabled	
9	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.9	10000	Point-to-Point	Disabled	Disabled	
10	Enabled	Discarding	0	10000	32768.0030F1D473A0	128.10	10000	Point-to-Point	Disabled	Disabled	

Figure 10-3 STA Port Information

CLI – This example shows the STA attributes for port 5.

```
Console#show spanning-tree ethernet 1/5                             33-18
Eth   1/ 5 information
--------------------------------------------------------------
 Admin Status:                Enabled
 Role:                        disable
 State:                       discarding
 External Admin Path Cost: 0
 Internal Admin Path Cost: 0
 External Oper Path Cost:  10000
 Internal Oper Path Cost:  10000
 Priority:                    128
 Designated Cost:             100000
 Designated Port:             128.5
 Designated Root:              32768.0.0001ECF8D8C6
 Designated Bridge:            32768.0.123411114321
 Fast Forwarding:             Disabled
 Forward Transitions:        0
 Admin Edge Port:             Disabled
 Oper Edge Port:              Disabled
 Admin Link Type:             auto
 Oper Link Type:               Point-to-point
 Spanning Tree Status:        Enabled

Console#
```

Configuring Interface Settings

You can configure RSTP and MSTP attributes for specific interfaces, including port priority, path cost, link type, and edge port. You may use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 10-10 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk**[11] – Indicates if a port is a member of a trunk.

[11] STA Port Configuration only

The following interface attributes can be configured:

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
  - Default: 128
  - Range: 0-240, in steps of 16
- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

Table 10-4 Recommended STA Path Cost Range

Port Type	Short Path Cost* (IEEE 802.1D-1998)	Long Path Cost* (802.1D-2004)
Gigabit Ethernet	2,000-65,535	2,000-200,000
10G Ethernet	200-20,000	200-20,000

* Use the STA Configuration screen (page 10-6) to set the path cost method.

Table 10-5 Default STA Path Costs

Port Type	Short Path Cost* (IEEE 802.1D-1998)	Long Path Cost* (802.1D-2004)
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

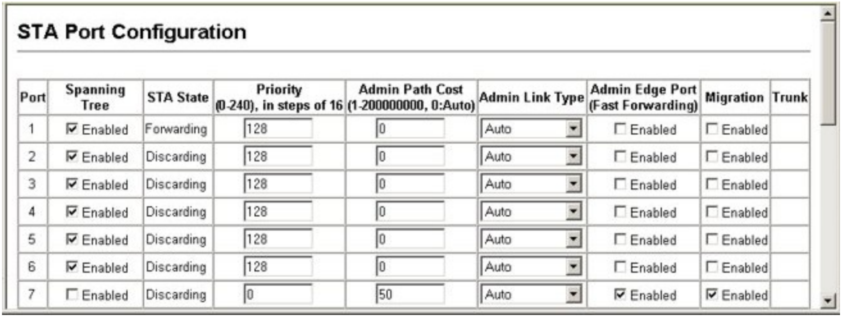
* Use the STA Configuration screen (page 10-6) to set the path cost method.

- **Admin Link Type** – The link type attached to this interface.
  - Point-to-Point – A connection to exactly one other bridge.
  - Shared – A connection to two or more bridges.
  - Auto – The switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port** (Fast Forwarding) – You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current

forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)

- **Migration** – If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the Protocol Migration button to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Web – Click Spanning Tree, STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.



STA Port Configuration

Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Admin Path Cost (1-200000000, 0:Auto)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	☑ Enabled	Forwarding	128	0	Auto	□ Enabled	□ Enabled	
2	☑ Enabled	Discarding	128	0	Auto	□ Enabled	□ Enabled	
3	☑ Enabled	Discarding	128	0	Auto	□ Enabled	□ Enabled	
4	☑ Enabled	Discarding	128	0	Auto	□ Enabled	□ Enabled	
5	☑ Enabled	Discarding	128	0	Auto	□ Enabled	□ Enabled	
6	☑ Enabled	Discarding	128	0	Auto	□ Enabled	□ Enabled	
7	□ Enabled	Discarding	0	50	Auto	☑ Enabled	☑ Enabled	

Figure 10-6 STA Port Configuration

CLI – This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7                              27-1
Console(config-if)#no spanning-tree spanning-disabled              33-11
Console(config-if)#spanning-tree port-priority 0                   33-13
Console(config-if)#spanning-tree cost 50                           33-12
Console(config-if)#spanning-tree link-type auto                    33-15
Console(config-if)#no spanning-tree edge-port                      33-13
Console(config-if)#spanning-tree protocol-migration                33-17
Console(config-if)#
```

Configuring Multiple Spanning Trees

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. This switch supports up to 33 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 10-8) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (STA Configuration, page 10-6).
2. Enter the spanning tree priority for the selected MST instance (MSTP VLAN Configuration).
3. Add the VLANs that will share this MSTI (MSTP VLAN Configuration).

Note: All VLANs are automatically added to the IST (Instance 0).

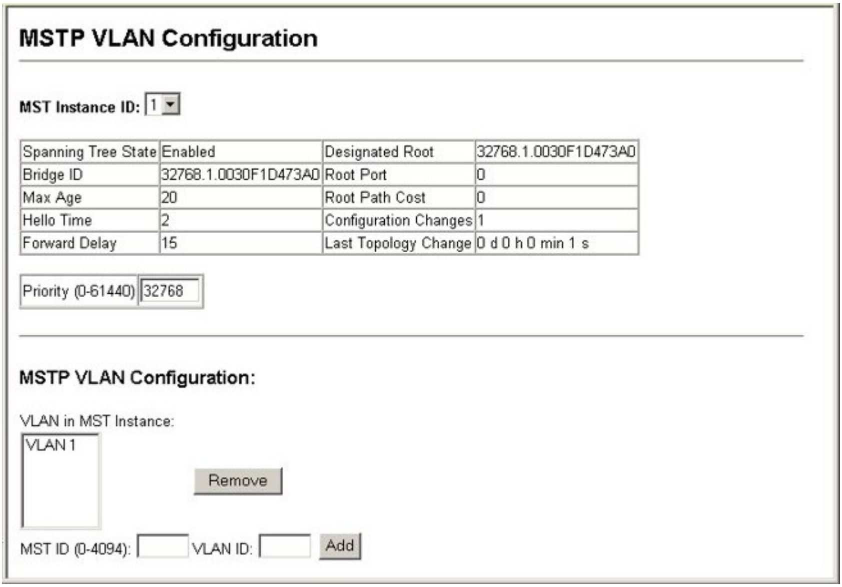
To ensure that the MSTI maintains connectivity across the network, you must configure a related set of bridges with the same MSTI settings.

Command Attributes

- **MST Instance** – Instance identifier of this spanning tree. (Default: 0)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)
- **VLANs in MST Instance** – VLANs assigned this instance.
- **MST ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **VLAN ID** – VLAN to assign to this selected MST instance. (Range: 1-4093)

The other global attributes are described under “Displaying Global Settings,” page 10-3. The attributes displayed by the CLI for individual interfaces are described under “Displaying Interface Settings,” page 10-10

Web – Click Spanning Tree, MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.



MSTP VLAN Configuration

MST Instance ID: 1

Spanning Tree State	Enabled	Designated Root	32768.1.0030F1D473A0
Bridge ID	32768.1.0030F1D473A0	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 1 s

Priority (0-61440) 32768

MSTP VLAN Configuration:

VLAN in MST Instance:

VLAN 1

MST ID (0-4094): VLAN ID:

Figure 10-7 MSTP VLAN Configuration

CLI – This displays STA settings for instance 1, followed by settings for each port.

```
Console#show spanning-tree mst 1                                        33-18
Spanning-tree information
-------------------------------------------------------------------
 Spanning Tree Mode:                   MSTP
 Spanning Tree Enabled/Disabled:        Enabled
 Instance:                             1
 VLANs Configuration:                  1
 Priority:                             32768
 Bridge Hello Time (sec.):             2
 Bridge Max Age (sec.):                20
 Bridge Forward Delay (sec.):          15
 Root Hello Time (sec.):               2
 Root Max Age (sec.):                  20
 Root Forward Delay (sec.):            15
 Max  Hops:                            20
 Remaining Hops:                       20
 Designated Root:                        32768.1.0000E8900000
 Current Root Port:                    0
 Current Root Cost:                    0
 Number of Topology Changes:           1
 Last Topology Change Time (sec.):     47
 Transmission Limit:                   3
 Path Cost Method:                     Long
```

```
---------------------------------------------------------------
Eth   1/ 7 information
---------------------------------------------------------------
 Admin Status:                Enabled
 Role:                        designate
 State:                       forwarding
 External Admin Path Cost: 0
 Internal Admin Path Cost: 0
 External Oper Path Cost:  10000
 Internal Oper Path Cost:  10000
 Priority:                 128
 Designated Cost:          0
 Designated Port:          128.23
 Designated Root:          32768.1.0000E8900000
 Designated Bridge:        32768.1.0000E8900000
 Fast Forwarding:          Disabled
 Forward Transitions:      2
 Admin Edge Port:          Disabled
 Oper Edge Port:           Disabled
 Admin Link Type:          auto
 Oper Link Type:           Point-to-point
 Spanning Tree Status:     Enabled
 ⋮
```

CLI – This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

```
Console(config)#spanning-tree mst-configuration                      33-7
Console(config-mst)#mst 1 priority 4096                              33-9
Console(config-mstp)#mst 1 vlan 1-5                                  33-8
Console(config-mst)#
```

Displaying Interface Settings for MSTP

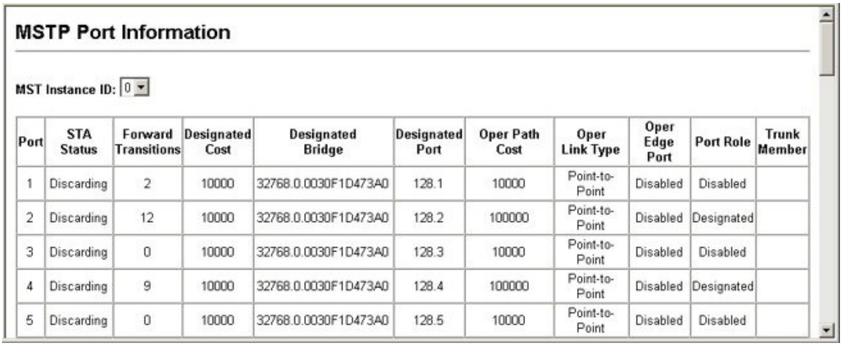
The MSTP Port Information and MSTP Trunk Information pages display the current status of ports and trunks in the selected MST instance.

Field Attributes

MST Instance ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

The other attributes are described under “Displaying Interface Settings,” page 10-10.

Web – Click Spanning Tree, MSTP, Port Information or Trunk Information. Select the required MST instance to display the current spanning tree values.



MSTP Port Information

MST Instance ID: 0

Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Discarding	2	10000	32768.0.0030F1D473A0	128.1	10000	Point-to-Point	Disabled	Disabled	
2	Discarding	12	10000	32768.0.0030F1D473A0	128.2	100000	Point-to-Point	Disabled	Designated	
3	Discarding	0	10000	32768.0.0030F1D473A0	128.3	10000	Point-to-Point	Disabled	Disabled	
4	Discarding	9	10000	32768.0.0030F1D473A0	128.4	100000	Point-to-Point	Disabled	Designated	
5	Discarding	0	10000	32768.0.0030F1D473A0	128.5	10000	Point-to-Point	Disabled	Disabled	

Figure 10-8 MSTP Port Information

CLI – This displays STA settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the IST (page 10-3), the settings for other instances only apply to the local spanning tree.

```
Console#show spanning-tree mst 0                                      33-18
Spanning-tree information
-------------------------------------------------------------------
 Spanning Tree Mode:                   MSTP
 Spanning Tree Enabled/Disabled:       Enabled
 Instance:                             0
 VLANs Configuration:                  2-4093
 Priority:                             32768
 Bridge Hello Time (sec.):             2
 Bridge Max Age (sec.):                20
 Bridge Forward Delay (sec.):          15
 Root Hello Time (sec.):               2
 Root Max Age (sec.):                  20
 Root Forward Delay (sec.):            15
 Max  Hops:                            20
 Remaining Hops:                       20
 Designated Root:                       32768.0.0000E8900000
 Current Root Port:                    0
 Current Root Cost:                    0
 Number of Topology Changes:           5
 Last Topology Change Time (sec.): 127
 Transmission Limit:                   3
 Path Cost Method:                     Long
```

```
---------------------------------------------------------------
Eth   1/ 1 information
---------------------------------------------------------------
 Admin Status:                Enabled
 Role:                        designate
 State:                       forwarding
 External Admin Path Cost: 0
 Internal Admin Path Cost: 0
 External Oper Path Cost:  10000
 Internal Oper Path Cost:  10000
 Priority:                 128
 Designated Cost:          0
 Designated Port:          128.23
 Designated Root:          32768.0.0000E8900000
 Designated Bridge:        32768.0.0000E8900000
 Fast Forwarding:          Disabled
 Forward Transitions:      4
 Admin Edge Port:          Disabled
 Oper Edge Port:           Disabled
 Admin Link Type:          auto
 Oper Link Type:           Point-to-point
 Spanning Tree Status:     Enabled
:
```

Configuring Interface Settings for MSTP

You can configure the STA interface settings for an MST Instance using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 10-10 for additional information.)
  - **Discarding** - Port receives STA configuration messages, but does not forward packets.
  - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
  - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree

Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

- Default: 128
- Range: 0-240, in steps of 16

- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 3-63), the maximum path cost is 65,535.

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost "0" is used to indicate auto-configuration mode.

Table 10-9 Recommended STA Path Cost Range

Port Type	Short Path Cost* (IEEE 802.1D-1998)	Long Path Cost* (802.1D-2004)
Gigabit Ethernet	2,000-65,535	2,000-200,000
10G Ethernet	200-20,000	200-20,000

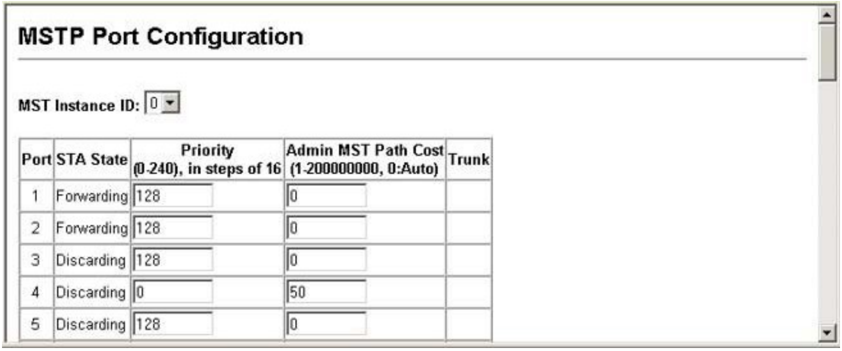
* Use the STA Configuration screen (page 10-6) to set the path cost method.

Table 10-10 Default STA Path Costs

Port Type	Short Path Cost* (IEEE 802.1D-1998)	Long Path Cost* (802.1D-2004)
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

* Use the STA Configuration screen (page 10-6) to set the path cost method.

Web – Click Spanning Tree, MSTP, Port Configuration or Trunk Configuration. Enter the priority and path cost for an interface, and click Apply.



MSTP Port Configuration

MST Instance ID: 0

Port	STA State	Priority (0-240), in steps of 16	Admin MST Path Cost (1-200000000, 0:Auto)	Trunk
1	Forwarding	128	0	
2	Forwarding	128	0	
3	Discarding	128	0	
4	Discarding	0	50	
5	Discarding	128	0	

Figure 10-11 MSTP Port Configuration

CLI – This example sets the MSTP attributes for port 4.

```
Console(config)#interface ethernet 1/4                              27-1
Console(config-if)#spanning-tree mst port-priority 0               33-17
Console(config-if)#spanning-tree mst cost 50                       33-16
Console(config-if)
```

Chapter 11: VLAN Configuration

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

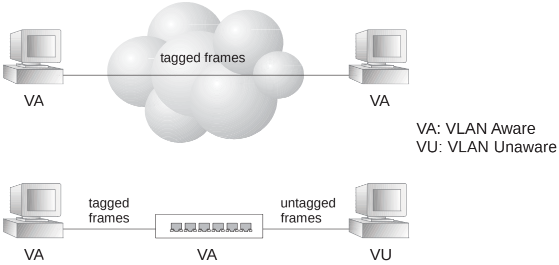
This switch supports the following VLAN features:

- Up to 4093 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.



VLAN Classification – When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

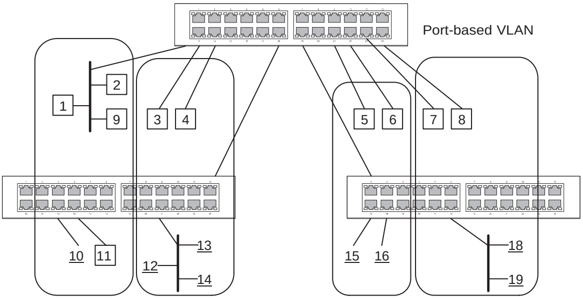
Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, you should use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to your network indicating the VLAN groups it wants to join. When this switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. You should also determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If you have host devices that do not support GVRP, you should configure static or untagged VLANs for the switch ports connected to these devices (as described in “Adding Static Members to VLANs (VLAN Index)” on page 11-7). But you can still enable GVRP on these edge switches, as well as on the core switches in the network.



Forwarding Tagged/Untagged Frames

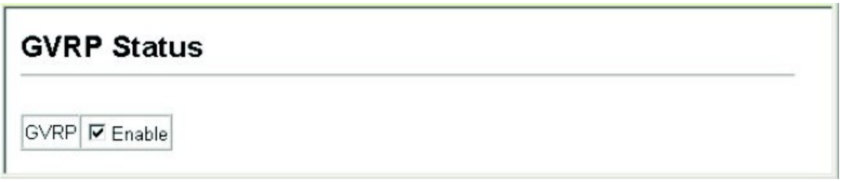
If you want to create a small port-based VLAN for devices attached directly to a single switch, you can assign ports to the same untagged VLAN. However, to participate in a VLAN group that crosses several switches, you should create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch must first strip off the VLAN tag before forwarding the frame. When the switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when this switch receives an untagged frame from a VLAN-unaware device, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port’s default VID.

Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Web – Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, click Apply



GVRP Status

GVRP ☑ Enable

Figure 11-1 Globally Enabling GVRP

CLI – This example enables GVRP for the switch.

```
Console(config)#bridge-ext gvrp                                       34-2
Console(config)#
```

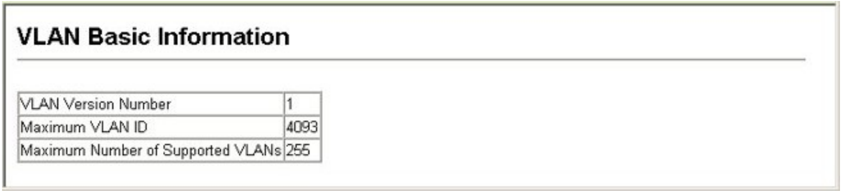
Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the switch.

Field Attributes

- **VLAN Version Number**[12] – The VLAN version used by this switch as specified in the IEEE 802.1Q standard.
- **Maximum VLAN ID** – Maximum VLAN ID recognized by this switch.
- **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on this switch.

Web – Click VLAN, 802.1Q VLAN, Basic Information.



VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4093
Maximum Number of Supported VLANs	255

Figure 11-2 VLAN Basic Information

[12] Web Only.

CLI – Enter the following command.

```
Console#show bridge-ext                                                   34-2
 Max support VLAN numbers:                  4096
 Max support VLAN ID:                       4093
 Extended multicast filtering services: No
 Static entry individual port:              Yes
 VLAN  learning:                            IVL
 Configurable PVID tagging:                 Yes
 Local VLAN capable:                        No
 Traffic classes:                           Enabled
 Global GVRP status:                        Disabled
 GMRP:                                      Disabled
Console#
```

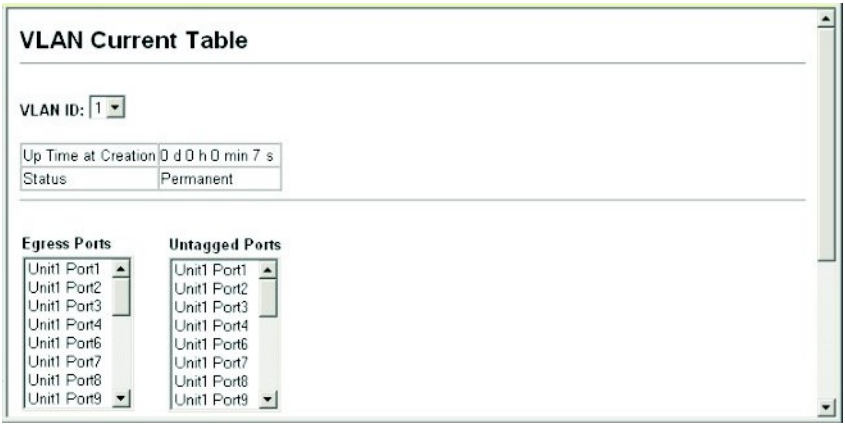
Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, if you just want to create a small port-based VLAN for one or two switches, you can disable tagging.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4093).
- **Up Time at Creation** – Time this VLAN was created (i.e., System Up Time).
- **Status** – Shows how this VLAN was added to the switch.
  - **Dynamic GVRP**: Automatically learned via GVRP.
  - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.



VLAN Current Table

VLAN ID: 1

Up Time at Creation	0 d 0 h 0 min 7 s
Status	Permanent

Egress Ports

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port6
Unit1 Port7
Unit1 Port8
Unit1 Port9

Untagged Ports

Unit1 Port1
Unit1 Port2
Unit1 Port3
Unit1 Port4
Unit1 Port6
Unit1 Port7
Unit1 Port8
Unit1 Port9

Figure 11-3 VLAN Current Table

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4093, no leading zeroes).
- **Type** – Shows how this VLAN was added to the switch.
  - **Dynamic**: Automatically learned via GVRP.
  - **Static**: Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

```
Console#show vlan id 1                                                  34-13

VLAN ID:                 1
Type:                    Static
Name:                    DefaultVlan
Status:                  Active
Ports/Port Channels:     Eth2/ 1(S) Eth2/ 2(S) Eth2/ 3(S) Eth2/ 4(S) Eth2/ 5(S)
                         Eth2/ 6(S) Eth2/ 7(S) Eth2/ 8(S) Eth2/ 9(S) Eth2/10(S)
                         Eth2/11(S) Eth2/12(S) Eth2/13(S) Eth2/14(S) Eth2/15(S)
                         Eth2/16(S) Eth2/17(S) Eth2/18(S) Eth2/19(S) Eth2/20(S)
                         Eth2/21(S) Eth2/22(S) Eth2/23(S) Eth2/24(S) Eth2/25(S)
                         Eth2/26(S)
Console#
```

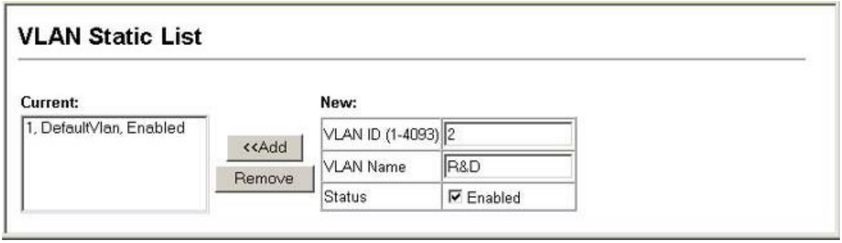
Creating VLANs

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on this switch to external network devices, you must specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 4093 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.
- **New** – Allows you to specify the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4093).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status** (Web) – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **State** (CLI) – Enables or disables the specified VLAN.
  - **Active**: VLAN is operational.
  - **Suspend**: VLAN is suspended; i.e., does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.



VLAN Static List

Current:

1, DefaultVlan, Enabled

New:

VLAN ID (1-4093): 2

VLAN Name: R&D

Status: ☑ Enabled

Figure 11-4 VLAN Static List - Creating VLANs

CLI – This example creates a new VLAN.

```
Console(config)#vlan database                                         34-5
Console(config-vlan)#vlan 2 name R&D media ethernet state active      34-6
Console(config-vlan)#end
Console#show vlan                                                     34-13

VLAN ID:                1
Type:                   Static
Name:                   DefaultVlan
Status:                 Active
Ports/Port Channels:    Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                        Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                        Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                        Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                        Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S)
:
VLAN ID:                2
Type:                   Static
Name:                   R&D
Status:                 Active
Ports/Port Channels:

Console#
```

Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-aware devices. Or configure a port as forbidden to prevent the switch from automatically adding it to a VLAN via the GVRP protocol.

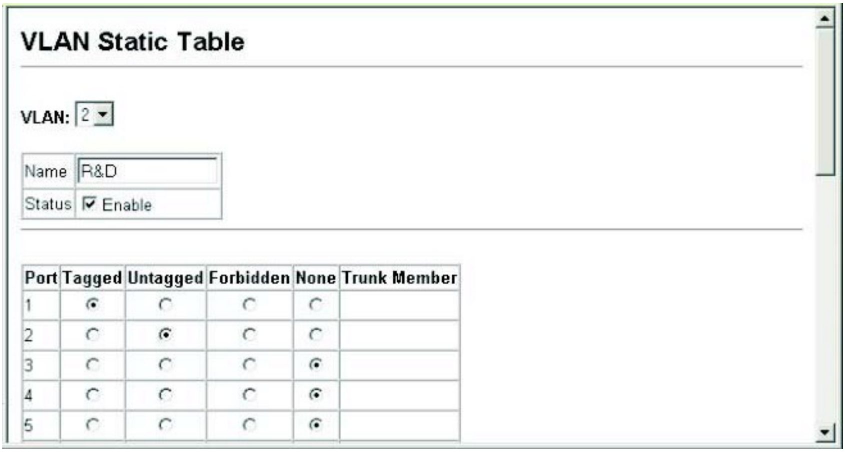
Notes:

1. You can also use the VLAN Static Membership by Port page to configure VLAN groups based on the port index (page 9). However, note that this configuration page can only add ports to a VLAN as tagged members.
2. VLAN 1 is the default untagged VLAN containing all ports on the switch, and can only be modified by first reassigning the default port VLAN ID as described under “Configuring VLAN Behavior for Interfaces” on page 11-10.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4093).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
  - **Enable**: VLAN is operational.
  - **Disable**: VLAN is suspended; i.e., does not pass packets.
- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- **Membership Type** – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Forbidden**: Interface is forbidden from automatically joining the VLAN via GVRP. For more information, see "Automatic VLAN Registration" on page 11-2.
  - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.



VLAN Static Table

VLAN: 2

Name	R&D
Status	☑ Enable

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	●	○	○	○	
2	○	●	○	○	
3	○	○	○	●	
4	○	○	○	●	
5	○	○	○	●	

Figure 11-5 VLAN Static Table - Adding Static Members

CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1                               27-1
Console(config-if)#switchport allowed vlan add 2 tagged             34-11
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#
```

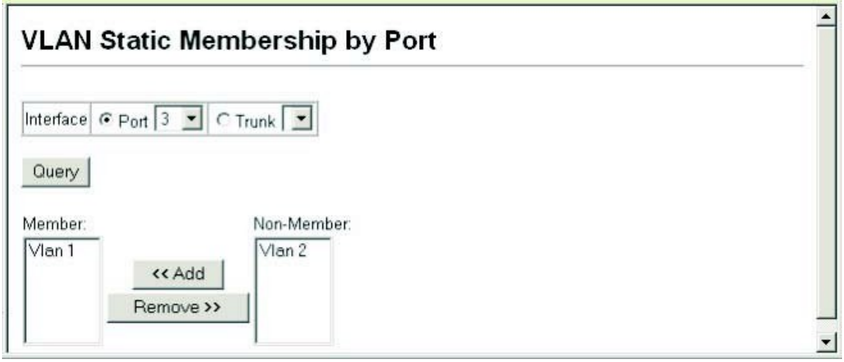
Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.
- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, 802.1Q VLAN, Static Membership by Port. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.



VLAN Static Membership by Port

Interface ● Port 3 ○ Trunk

Member: Vlan 1

Non-Member: Vlan 2

Figure 11-6 VLAN Static Membership by Port

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3                               27-1
Console(config-if)#switchport allowed vlan add 1 tagged             34-11
Console(config-if)#switchport allowed vlan remove 2
Console(config-if)#
```

Configuring VLAN Behavior for Interfaces

You can configure VLAN behavior for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.
- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GVRP registration/deregistration.

Command Attributes

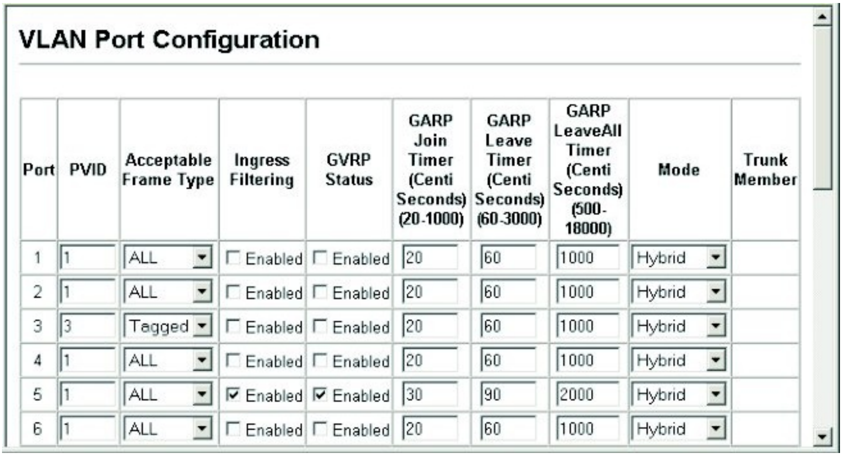
- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
  - If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)
  - Ingress filtering only affects tagged frames.
  - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
  - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
  - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the switch before this setting can take effect. (See “Displaying Bridge Extension Capabilities” on page 4-4.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)
- **GARP Join Timer**[13] – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave Timer**[13] – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a

[13] Timer settings must follow this rule: 2 x (join timer) < leave timer < leaveAll timer

Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)

- **GARP LeaveAll Timer**[13] – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group.
  (Range: 500-18000 centiseconds; Default: 1000)
- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
  - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.
  - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration. Fill in the required settings for each interface, click Apply.



VLAN Port Configuration

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	Trunk Member
1	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	
2	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	
3	3	Tagged	□ Enabled	□ Enabled	20	60	1000	Hybrid	
4	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	
5	1	ALL	☑ Enabled	☑ Enabled	30	90	2000	Hybrid	
6	1	ALL	□ Enabled	□ Enabled	20	60	1000	Hybrid	

Figure 11-7 VLAN Port Configuration

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```
Console(config)#interface ethernet 1/3                              27-1
Console(config-if)#switchport acceptable-frame-types tagged         34-9
Console(config-if)#switchport ingress-filtering                     34-9
Console(config-if)#switchport native vlan 3                        34-10
Console(config-if)#switchport gvrp                                  34-3
Console(config-if)#garp timer join 20                               34-4
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid                           34-8
Console(config-if)#
```

Configuring IEEE 802.1Q Tunneling

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer’s frames when they enter the service provider’s network, and then stripping the tags when the frames leave the network.

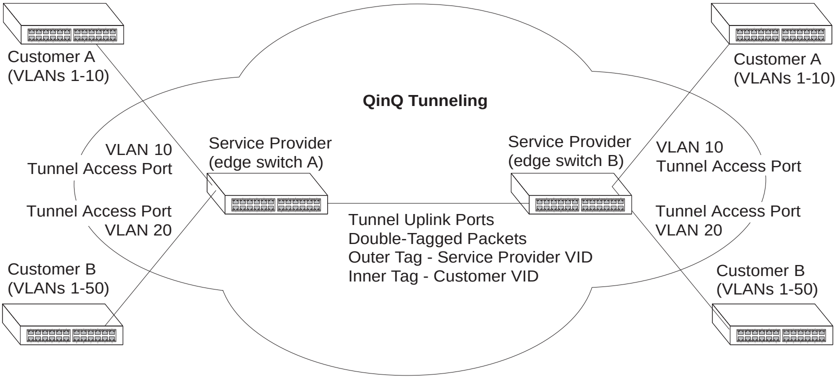
A service provider’s customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider’s network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer’s original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider’s network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider’s metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider’s network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider’s network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider’s egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer’s network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer’s network.



Layer 2 Flow for Packets Coming into a Tunnel Access Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. New SPVLAN tags are added to all incoming packets, no matter how many tags they already have. The ingress process constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag). This outer tag is used for learning and switching packets. The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.
2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag (8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.

3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).
4. The switch sends the packet to the proper egress port.
5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into a Tunnel Uplink Port

An uplink port receives one of the following packets:

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port’s PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider’s network. The TPID must be configured on a per port basis, and the verification cannot be disabled.
3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookups, the packet is double tagged. The switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.
5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The switch sends the packet to the proper egress port.
8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

- The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes non-customer packets to be forwarded to the SPVLAN.
- Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.
- The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoid using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.
- There are some inherent incompatibilities between Layer 2 and Layer 3 switching:
  - Tunnel ports do not support IP Access Control Lists.
  - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
  - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (see “Enabling QinQ Tunneling on the Switch” on page 11-16).
2. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The default ethertype value is 0x8100. (See “Adding an Interface to a QinQ Tunnel” on page 11-17.)
3. Create a Service Provider VLAN, also referred to as an SPVLAN (see “Creating VLANs” on page 11-6).
4. Configure the QinQ tunnel access port to 802.1Q Tunnel mode (see “Adding an Interface to a QinQ Tunnel” on page 11-17).
5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (see “Adding Static Members to VLANs (VLAN Index)” on page 11-7).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (see “Configuring VLAN Behavior for Interfaces” on page 11-10).
7. Configure the QinQ tunnel uplink port to 802.1Q Tunnel Uplink mode (see “Adding an Interface to a QinQ Tunnel” on page 11-17).
8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (see “Adding Static Members to VLANs (VLAN Index)” on page 11-7).

Enabling QinQ Tunneling on the Switch

The switch can be configured to operate in normal VLAN mode or IEEE 802.1Q (QinQ) tunneling mode which is used for passing Layer 2 traffic across a service provider's metropolitan area network. You can also globally set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

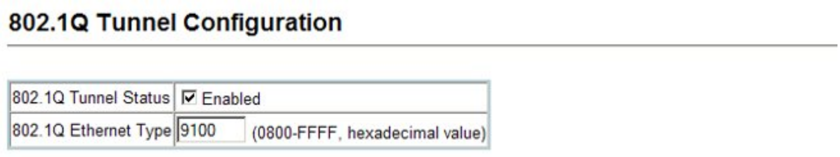
Command Usage

- Use the TPID field to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, if 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.
- All ports on the switch will be set to the same ethertype.

Command Attributes

- **802.1Q Tunnel Status** – Sets the switch to QinQ mode, and allows the QinQ tunnel port to be configured. The default is for the switch to function in normal mode.
- **802.1Q Ethernet Type** – The Tag Protocol Identifier (TPID) specifies the ethertype of incoming packets on a tunnel port. (Range: hexadecimal 0800-FFFF; Default: 8100)

Web – Click VLAN, 802.1Q VLAN, 802.1Q Tunnel Configuration. Check the Enabled box, set the TPID of the ports if the client is using a non-standard ethertype to identify 802.1Q tagged frames, and click Apply.



802.1Q Tunnel Configuration

802.1Q Tunnel Status	☑ Enabled
802.1Q Ethernet Type	9100 (0800-FFFF, hexadecimal value)

Figure 11-1 802.1Q Tunnel Status and Ethernet Type

CLI – This example sets the switch to operate in QinQ mode.

```
Console(config)#dot1q-tunnel system-tunnel-control                    34-15
Console(config-if)#switchport dot1q-tunnel tpid 9100                  34-16
Console(config)#exit
Console#show dot1q-tunnel                                             34-17

Current double-tagged status of the system is Enabled

The dot1q-tunnel mode of the set interface 1/1 is Access mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/4 is Normal mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/5 is Normal mode, TPID is 0x9100.
⋮
```

Adding an Interface to a QinQ Tunnel

Follow the guidelines in the preceding section to set up a QinQ tunnel on the switch. Use the VLAN Port Configuration or VLAN Trunk Configuration screen to set the access port on the edge switch to 802.1Q Tunnel mode.

Command Usage

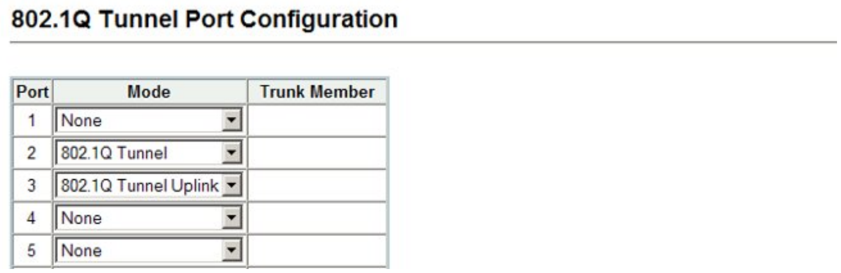
- Use the 802.1Q Tunnel Status screen to set the switch to QinQ mode before configuring a tunnel port (see “Enabling QinQ Tunneling on the Switch” on page 11-16). Also set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames (see “Enabling QinQ Tunneling on the Switch” on page 11-16).
- Set the mode to 802.1Q Tunnel (access) or 802.1Q Tunnel Uplink.

Command Attributes

Mode – Set the VLAN membership mode of the port.

- **None** – The port operates in its normal VLAN mode. (This is the default.)
- **802.1Q Tunnel** – Configures IEEE 802.1Q tunneling (QinQ) for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
- **802.1Q Tunnel Uplink** – Configures IEEE 802.1Q tunneling (QinQ) for an uplink port to another device within the service provider network.
- **Trunk Member** – Shows if a port is a member or a trunk.

Web – Click VLAN, 802.1Q VLAN, 802.1Q Tunnel Configuration or Tunnel Trunk Configuration. Set the mode for a tunnel access port to 802.1Q Tunnel and a tunnel uplink port to 802.1Q Tunnel Uplink. Click Apply.



802.1Q Tunnel Port Configuration

Port	Mode	Trunk Member
1	None	
2	802.1Q Tunnel	
3	802.1Q Tunnel Uplink	
4	None	
5	None	

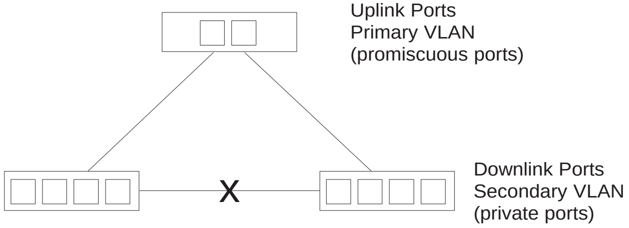
Figure 11-2 Tunnel Port Configuration

CLI – This example sets port 2 to tunnel access mode, and sets port 3 to tunnel uplink mode.

```
Console(config)#interface ethernet 1/2                               27-1
Console(config-if)#switchport dot1q-tunnel mode access              34-15
Console(config-if)#interface ethernet 1/3
Console(config-if)#switchport dot1q-tunnel mode uplink              34-15
Console(config-if)#end
Console#show dot1q-tunnel                                           34-17

Current double-tagged status of the system is Enabled
The dot1q-tunnel mode of the set interface 1/1 is Normal mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/2 is Access mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/3 is Uplink mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/4 is Normal mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/5 is Normal mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/6 is Normal mode, TPID is 0x9100.
The dot1q-tunnel mode of the set interface 1/7 is Normal mode, TPID is 0x9100.
:
```

Configuring Private VLANs

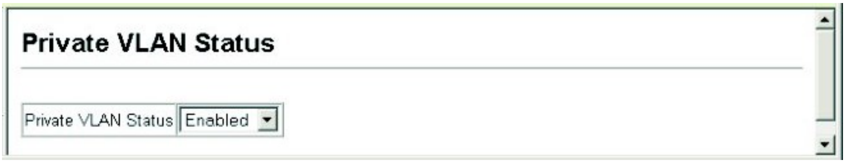
Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports. (Note that private VLANs and normal VLANs can exist simultaneously within the same switch.)



Enabling Private VLANs

Use the Private VLAN Status page to enable/disable the Private VLAN function.

Web – Click VLAN, Private VLAN, Status. Select Enable or Disable from the scroll-down box, and click Apply.



Private VLAN Status

Private VLAN Status: Enabled

Figure 11-8 Private VLAN Status

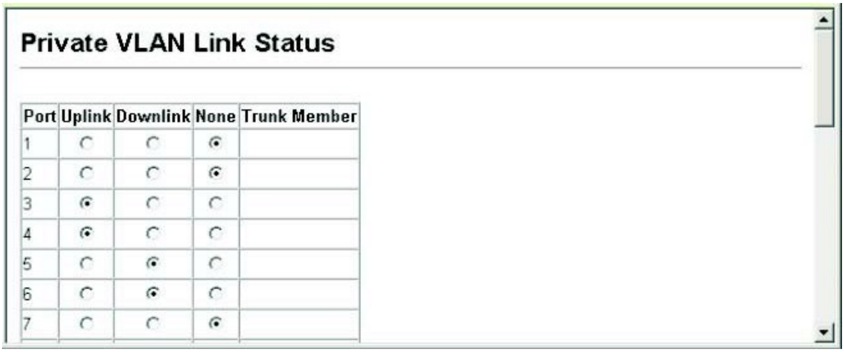
CLI – This example enables private VLANs.

```
Console(config)#pvlan                                              34-18
Console(config)#
```

Configuring Uplink and Downlink Ports

Use the Private VLAN Link Status page to set ports as downlink or uplink ports. Ports designated as downlink ports can not communicate with any other ports on the switch except for the uplink ports. Uplink ports can communicate with any other ports on the switch and with any designated downlink ports.

Web – Click VLAN, Private VLAN, Link Status. Mark the ports that will serve as uplinks and downlinks for the private VLAN, then click Apply.



Private VLAN Link Status

Port	Uplink	Downlink	None	Trunk Member
1	○	○	●	
2	○	○	●	
3	●	○	○	
4	●	○	○	
5	○	●	○	
6	○	●	○	
7	○	○	●	

Figure 11-9 Private VLAN Link Status

CLI – This configures port 3 as an uplink and port 5 and 6 as downlinks.

```
Console(config)#pvlan up-link ethernet 1/3 down-link ethernet 1/5    34-18
Console(config)#pvlan up-link ethernet 1/3 down-link ethernet 1/6
Console(config)#end
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/3
Down-link port:
 Ethernet 1/5
 Ethernet 1/6
Console#
```

Configuring Protocol-Based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 6). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the Protocol VLAN Configuration page.
3. Then map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

Configuring Protocol Groups

Create a protocol group for one or more protocols.

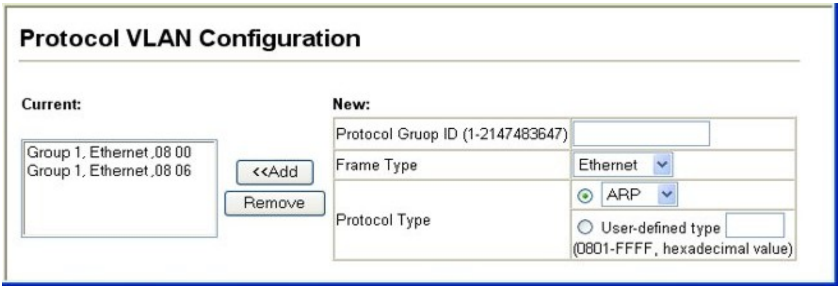
Command Attributes

- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **Frame Type**[14] – Frame type used by this protocol. (Options: Ethernet, RFC_1042, LLC_other)

[14] SNAP frame types are not supported by this switch due to hardware limitations.

- **Protocol Type** – The only option for the LLC_other frame type is IPX_raw. The options for all other frames types include: IP, IPv6, ARP, RARP, and user-defined (0801-FFFF hexadecimal).

Web – Click VLAN, Protocol VLAN, Configuration. Enter a protocol group ID, frame type and protocol type, then click Apply.



Protocol VLAN Configuration

Current:

Group 1, Ethernet,08 00
Group 1, Ethernet,08 06

New:

Protocol Gruop ID (1-2147483647)	
Frame Type	Ethernet
Protocol Type	● ARP ○ User-defined type (0801-FFFF, hexadecimal value)

Figure 11-10 Protocol VLAN Configuration

CLI – The following creates protocol group 1, and then specifies Ethernet frames with IP and ARP protocol types.

```
Console(config)#protocol-vlan protocol-group 1
 add frame-type ethernet protocol-type ip                    34-20
Console(config)#protocol-vlan protocol-group 1
 add frame-type ethernet protocol-type arp
Console(config)#
```

Mapping Protocols to VLANs

Map a protocol group to a VLAN for each interface that will participate in the group.

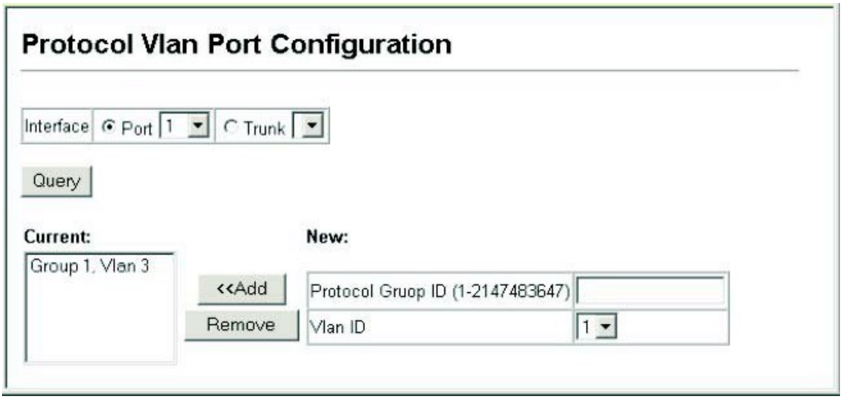
Command Usage

- When creating a protocol-based VLAN, only assign interfaces using this configuration screen. If you assign interfaces using any of the other VLAN menus such as the VLAN Static Table (page 7) or VLAN Static Membership by Port menu (page 9), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

Web – Click VLAN, Protocol VLAN, Port Configuration. Select a a port or trunk, enter a protocol group ID, the corresponding VLAN ID, and click Apply.



Protocol Vlan Port Configuration

Interface ● Port 1 ○ Trunk

Current:

Group 1, Vlan 3

New:

Protocol Gruop ID (1-2147483647)

Vlan ID 1

Figure 11-11 Protocol VLAN Port Configuration

CLI – The following maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 3.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 3          34-21
Console(config-if)#
```

Chapter 12: Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers. This information can be used by SNMP applications to simplify troubleshooting, enhance network management, and maintain an accurate network topology.

Setting Basic LLDP Timing Attributes

Use the LLDP Configuration screen to set attributes for general functions such as globally enabling LLDP on the switch, setting the message ageout time, and setting the frequency for broadcasting general advertisements or reports about changes in the LLDP MIB.

Command Attributes

- **LLDP** – Enables LLDP globally on the switch. (Default: Disabled)
- **Transmission Interval** – Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

  This attribute must comply with the following rule:

  (Transmission Interval * Hold Time Multiplier) ″ 65536, and

  Transmission Interval >= (4 * Delay Interval)
- **Hold Time Multiplier** – Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:
  (Transmission Interval * Holdtime Multiplier) ″ 65536.
  Therefore, the default TTL is 4*30 = 120 seconds.
- **Delay Interval** – Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables.
  (Range: 1-8192 seconds; Default: 2 seconds)

  The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

  This attribute must comply with the rule: (4 * Delay Interval) ″ Transmission Interval

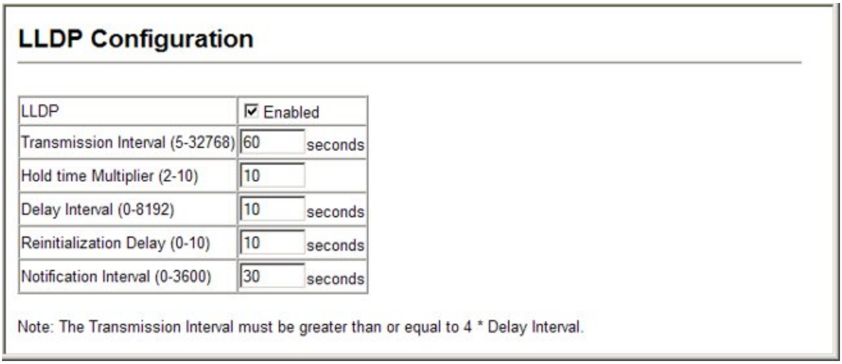
- **Reinitialization Delay** – Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. (Range: 1-10 seconds; Default: 2 seconds)

  When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.
- **Notification Interval** – Configures the allowed interval for sending SNMP notifications about LLDP MIB changes. (Range: 5-3600 seconds; Default: 5 seconds)

  This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.

  Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Web – Click LLDP, Configuration. Enable LLDP, modify any of the timing parameters as required, and click Apply.



LLDP Configuration

LLDP	☑ Enabled
Transmission Interval (5-32768)	60 seconds
Hold time Multiplier (2-10)	10
Delay Interval (0-8192)	10 seconds
Reinitialization Delay (0-10)	10 seconds
Notification Interval (0-3600)	30 seconds

Note: The Transmission Interval must be greater than or equal to 4 * Delay Interval.

Figure 12-4 LLDP Configuration

CLI – This example several attributes which control basic LLDP message timing.

```
Console(config)#lldp                                                     32-2
Console(config)#lldp refresh-interval 60                                 32-4
Console(config)#lldp holdtime-multiplier 10                              32-3
Console(config)#lldp tx-delay 10                                         32-5
Console(config)#lldp reinit-delay 10                                     32-5
Console(config)#lldp notification-interval 30                            32-3
Console(config)#exit
Console#show lldp config

LLDP Global Configuation

 LLDP Enable                  : Yes
 LLDP Transmit interval       : 60
 LLDP Hold Time Multiplier    : 10
 LLDP Delay Interval          : 10
 LLDP Reinit Delay            : 10
 LLDP Notification Interval   : 30
:
```

Configuring LLDP Interface Attributes

Use the LLDP Port/Trunk Configuration to specify the message attributes for individual interfaces, including whether messages are transmitted, received, or both transmitted and received, whether SNMP notifications are sent, and the type of information advertised.

Command Attributes

- **Admin Status** – Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Tx only, Rx only, RxTx, Disabled; Default: RxTx)
- **SNMP Notification** – Enables the transmission of SNMP trap notifications about LLDP changes. (Default: Disabled)

  This option sends out SNMP trap notifications to designated target stations at the interval specified by the Notification Interval in the preceding section. Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or vendor-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.

  For information on defining SNMP trap destinations, see “Specifying Trap Managers and Trap Types” on page 5-4.

  Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.
- **TLV Type** – Configures the information included in the TLV field of advertised messages.
  - **Port Description** – The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

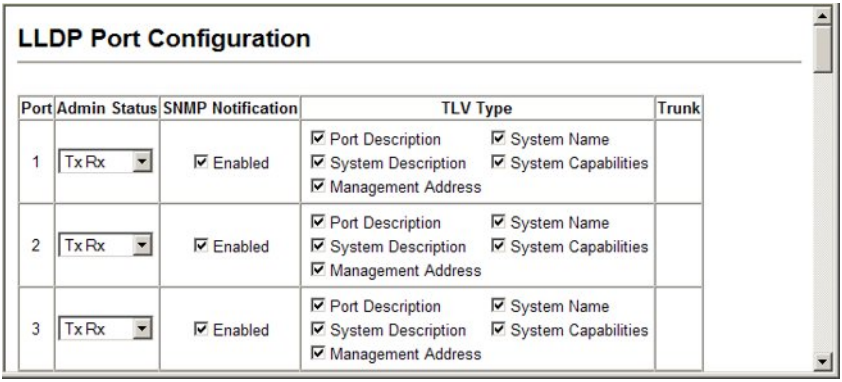
- **System Description** – The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.
- **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

  The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.

  Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

  Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.
- **System Name** – The system name is taken from the sysName object in RFC 3418, which contains the system’s administratively assigned name. To configure the system name, see “Displaying System Information” on page 4-1.
- **System Capabilities** – The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

Web – Click LLDP, Port/Trunk Configuration. Set the LLDP transmit/receive mode, specify whether or not to send SNMP trap messages, and select the information to advertise in LLDP messages. Then click Apply.



LLDP Port Configuration

Port	Admin Status	SNMP Notification	TLV Type	Trunk
1	Tx Rx	☑ Enabled	☑ Port Description ☑ System Name ☑ System Description ☑ System Capabilities ☑ Management Address	
2	Tx Rx	☑ Enabled	☑ Port Description ☑ System Name ☑ System Description ☑ System Capabilities ☑ Management Address	
3	Tx Rx	☑ Enabled	☑ Port Description ☑ System Name ☑ System Description ☑ System Capabilities ☑ Management Address	

Figure 12-5 LLDP Port Configuration

CLI – This example sets the interface to both transmit and receive LLDP messages, enables SNMP trap messages, and specifies the TLV parameters to advertise.

```
Console(config)#interface ethernet 1/1                                 27-1
Console(config-if)#lldp tx-rx                                          32-6
Console(config-if)#lldp notification                                   32-6
Console(config-if)#lldp basic-tlv port-description                     32-8
Console(config-if)#lldp basic-tlv system-description                   32-9
Console(config-if)#lldp basic-tlv management-ip-address                32-7
Console(config-if)#lldp basic-tlv system-name                          32-9
Console(config-if)#lldp basic-tlv system-capabilities                  32-8
Console(config-if)#
```

Displaying LLDP Local Device Information

Use the LLDP Local Device Information screen to display information about the switch, such as its MAC address, chassis ID, management IP address, and port information.

Field Attributes

Global Settings

- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field.

Table 12-1 Chassis ID Subtype

ID Basis	Reference
Chassis component	EntPhysicalAlias when entPhysClass has a value of ‘chassis(3)’ (IETF RFC 2737)
Interface alias	IfAlias (IETF RFC 2863)
Port component	EntPhysicalAlias when entPhysicalClass has a value ‘port(10)’ or ‘backplane(4)’ (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Locally assigned	locally assigned

- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **System Name** – An string that indicates the system’s administratively assigned name (see “Displaying System Information” on page 4-1).
- **System Description** – A textual description of the network entity. This field is also displayed by the **show system** command.

- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system.

Table 12-2 System Capabilities

ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

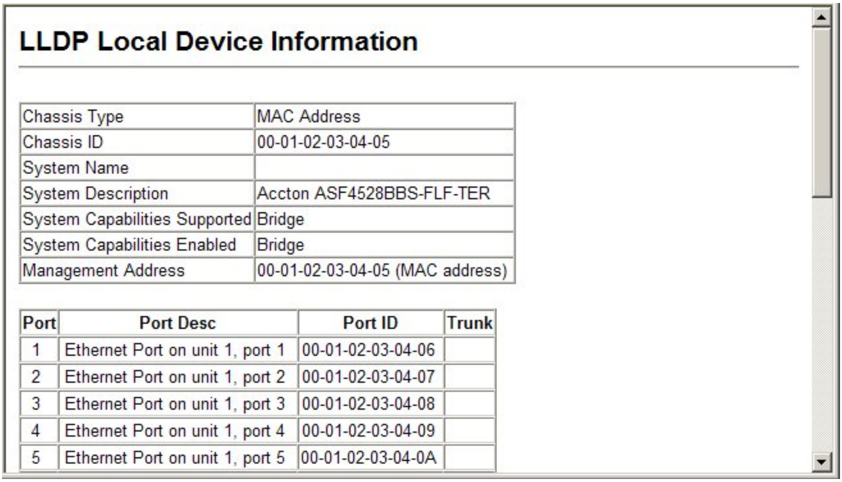
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table.
- **Management Address** – The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Interface Settings

The attributes listed below apply to both port and trunk interface types. When a trunk is listed, the descriptions apply to the first port of the trunk.

- **Port Description** – A string that indicates the port’s description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.

Web – Click LLDP, Local Information.



LLDP Local Device Information

Chassis Type	MAC Address
Chassis ID	00-01-02-03-04-05
System Name	
System Description	Accton ASF4528BBS-FLF-TER
System Capabilities Supported	Bridge
System Capabilities Enabled	Bridge
Management Address	00-01-02-03-04-05 (MAC address)

Port	Port Desc	Port ID	Trunk
1	Ethernet Port on unit 1, port 1	00-01-02-03-04-06	
2	Ethernet Port on unit 1, port 2	00-01-02-03-04-07	
3	Ethernet Port on unit 1, port 3	00-01-02-03-04-08	
4	Ethernet Port on unit 1, port 4	00-01-02-03-04-09	
5	Ethernet Port on unit 1, port 5	00-01-02-03-04-0A	

Figure 12-6 LLDP Local Device Information

CLI – This example displays LLDP information for the local switch.

```
Console#show lldp info local-device                                    32-15

 LLDP Local System Information
  Chassis Type : MAC Address
  Chassis ID     : 00-01-02-03-04-05
  System Name   :
  System Description : 24/48 port 10/100/1000 Stackable Managed Switch with
                       2 X 10G uplinks
  System Capabilities Support : Bridge
  System Capabilities Enable  : Bridge
  Management Address : 192.168.0.101 (IPv4)

 LLDP Port Information
 Interface |PortID Type      PortID             PortDesc
 --------- + ---------------- ----------------- ---------------------------
 Eth 1/1  |MAC Address    00-01-02-03-04-06 Ethernet Port on unit 1, port 1
 Eth 1/2  |MAC Address    00-01-02-03-04-07 Ethernet Port on unit 1, port 2
 Eth 1/3  |MAC Address    00-01-02-03-04-08 Ethernet Port on unit 1, port 3
 Eth 1/4  |MAC Address    00-01-02-03-04-09 Ethernet Port on unit 1, port 4
 Eth 1/5  |MAC Address    00-01-02-03-04-0A Ethernet Port on unit 1, port 5
 ⋮
```

This example displays detailed information for a specific port on the local switch.

```
Console#show lldp info local-device ethernet 1/1                         32-15

LLDP Port Information Detail

 Port       : Eth 1/1
 Port Type : MAC Address
 Port ID     : 00-01-02-03-04-06
 Port Desc : Ethernet Port on unit 1, port 1

Console#
```

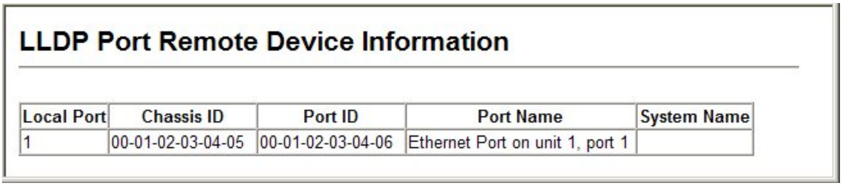
Displaying LLDP Remote Port Information

Use the LLDP Remote Port/Trunk Information screen to display information about devices connected directly to the switch’s ports which are advertising information through LLDP.

Field Attributes

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **Port Name** – A string that indicates the port’s description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **System Name** – An string that indicates the system’s administratively assigned name.

Web – Click LLDP, Remote Port/Trunk Information.



LLDP Port Remote Device Information

Local Port	Chassis ID	Port ID	Port Name	System Name
1	00-01-02-03-04-05	00-01-02-03-04-06	Ethernet Port on unit 1, port 1	

Figure 12-7 LLDP Remote Port Information

CLI – This example displays LLDP information for remote devices attached to this switch which are advertising information through LLDP.

```
Console#show lldp info remote-device                                      32-16

 LLDP Remote Devices Information

  Interface | ChassisId          PortId              SysName
  --------- + ----------------- ----------------- ---------------------
  Eth 1/1   | 00-01-02-03-04-05 00-01-02-03-04-06

Console#
```

Displaying LLDP Remote Information Details

Use the LLDP Remote Information Details screen to display detailed information about an LLDP-enabled device connected to a specific port on the local switch.

Field Attributes

- **Local Port** – The local port to which a remote LLDP-capable device is attached.
- **Chassis Type** – Identifies the chassis containing the IEEE 802 LAN entity associated with the transmitting LLDP agent. There are several ways in which a chassis may be identified and a chassis ID subtype is used to indicate the type of component being referenced by the chassis ID field. (See Table 12-1, “Chassis ID Subtype,” on page 12-5.)
- **Chassis ID** – An octet string indicating the specific identifier for the particular chassis in this system.
- **Port Type** – Indicates the basis for the identifier that is listed in the Port ID field.

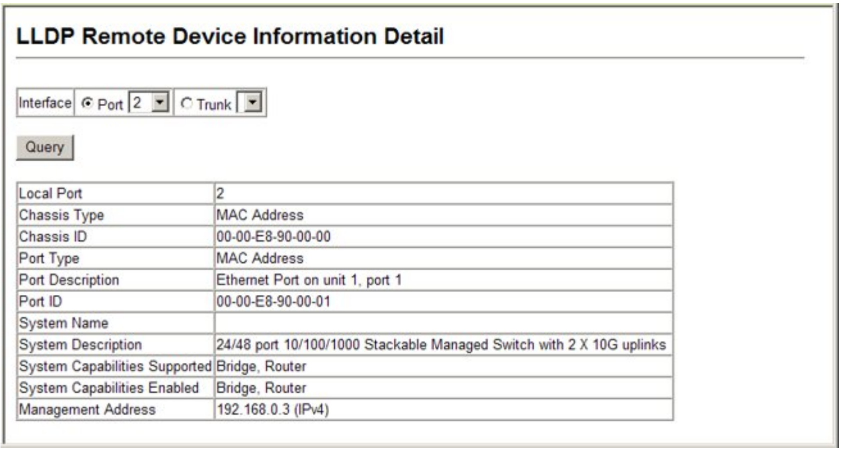
Table 12-3 Port ID Subtype

ID Basis	Reference
Interface alias	IfAlias (IETF RFC 2863)
Chassis component	EntPhysicalAlias when entPhysClass has a value of ‘chassis(3)’ (IETF RFC 2737)
Port component	EntPhysicalAlias when entPhysicalClass has a value ‘port(10)’ or ‘backplane(4)’ (IETF RFC 2737)
MAC address	MAC address (IEEE Std 802-2001)
Network address	networkAddress
Interface name	ifName (IETF RFC 2863)
Agent circuit ID	agent circuit ID (IETF RFC 3046)
Locally assigned	locally assigned

- **Port Description** – A string that indicates the port’s description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **Port ID** – A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **System Name** – An string that indicates the system’s configures assigned name.

- **System Description** – A textual description of the network entity.
- **System Capabilities Supported** – The capabilities that define the primary function(s) of the system. (See Table 12-2, “System Capabilities,” on page 12-6.)
- **System Capabilities Enabled** – The primary function(s) of the system which are currently enabled. Refer to the preceding table. (See Table 12-2, “System Capabilities,” on page 12-6.)
- **Management Address** – The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.

Web – Click LLDP, Remote Information Details. Select an interface from the drop down lists, and click Query.



LLDP Remote Device Information Detail

Interface ● Port 2 ○ Trunk

Local Port	2
Chassis Type	MAC Address
Chassis ID	00-00-E8-90-00-00
Port Type	MAC Address
Port Description	Ethernet Port on unit 1, port 1
Port ID	00-00-E8-90-00-01
System Name	
System Description	24/48 port 10/100/1000 Stackable Managed Switch with 2 X 10G uplinks
System Capabilities Supported	Bridge, Router
System Capabilities Enabled	Bridge, Router
Management Address	192.168.0.3 (IPv4)

Figure 12-8   LLDP Remote Information Details

CLI – This example displays LLDP information for an LLDP-enabled remote device attached to a specific port this switch.

```
Console#show lldp info remote-device detail ethernet 1/1                 32-16

 LLDP Remote Devices Information Detail

---------------------------------------------------------------
  Local PortName       : Eth 1/1
  Chassis Type         : MAC Address
  Chassis Id            : 00-01-02-03-04-05
  PortID Type          : MAC Address
  PortID                : 00-01-02-03-04-06
  SysName              :
  SysDescr                : 24/48 port 10/100/1000 Stackable Managed
                        Switch with 2 X 10G uplinks
  PortDescr               : Ethernet Port on unit 1, port 1
  SystemCapSupported : Bridge
  SystemCapEnabled     : Bridge
  Remote Management Address :
    00-01-02-03-04-05 (MAC Address)

Console#
```

Displaying Device Statistics

Use the LLDP Device Statistics screen to general statistics for LLDP-capable devices attached to the switch, and for LLDP protocol messages transmitted or received on all local interfaces.

Field Attributes

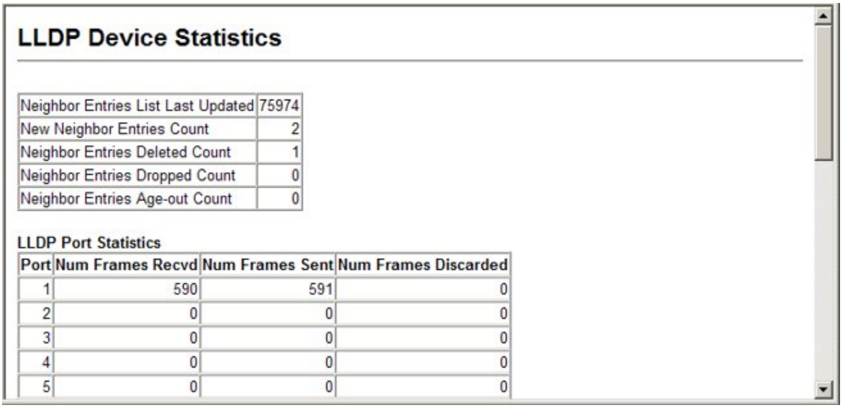
General Statistics on Remote Devices

- **Neighbor Entries List Last Updated** – The time the LLDP neighbor entry list was last updated.
- **New Neighbor Entries Count** – The number of LLDP neighbors for which the remote TTL has not yet expired.
- **Neighbor Entries Deleted Count** – The number of LLDP neighbors which have been removed from the LLDP remote systems MIB for any reason.
- **Neighbor Entries Dropped Count** – The number of times which the local remote database dropped an LLDPDU because of insufficient resources.
- **Neighbor Entries Age-out Count** – The number of times that a neighbor’s information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Interface Statistics on LLDP Protocol Messages

- **Num Frames Recvd** – Number of LLDP PDUs received.
- **Num Frames Sent** – Number of LLDP PDUs transmitted.
- **Num Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.

Web – Click LLDP, Device Statistics.



LLDP Device Statistics

Neighbor Entries List Last Updated	75974
New Neighbor Entries Count	2
Neighbor Entries Deleted Count	1
Neighbor Entries Dropped Count	0
Neighbor Entries Age-out Count	0

LLDP Port Statistics

Port	Num Frames Recvd	Num Frames Sent	Num Frames Discarded
1	590	591	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0

Figure 12-9 LLDP Device Statistics

CLI – This example displays LLDP statistics received from all LLDP-enabled remote devices connected directly to this switch.

```
switch#show lldp info statistics                                     32-18

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2450279 seconds
  New Neighbor Entries Count         : 1
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Interface | NumFramesRecvd NumFramesSent NumFramesDiscarded
  --------- + -------------- ------------- ------------------
  Eth 1/1   | 10             11            0
  Eth 1/2   | 0              0             0
  Eth 1/3   | 0              0             0
  Eth 1/4   | 0              0             0
  Eth 1/5   | 0              0             0
⋮
```

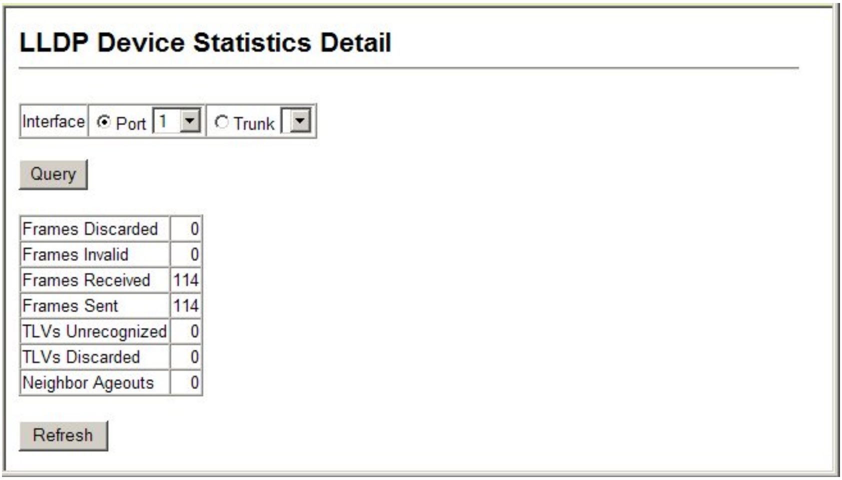
Displaying Detailed Device Statistics

Use the LLDP Device Statistics Details screen to display detailed statistics for LLDP-capable devices attached to specific interfaces on the switch.

Field Attributes

- **Frames Discarded** – Number of frames discarded because they did not conform to the general validation rules as well as any specific usage rules defined for the particular TLV.
- **Frames Invalid** – A count of all LLDPDUs received with one or more detectable errors.
- **Frames Received** – Number of LLDP PDUs received.
- **Frames Sent** – Number of LLDP PDUs transmitted.
- **TLVs Unrecognized** – A count of all TLVs not recognized by the receiving LLDP local agent.
- **TLVs Discarded** – A count of all LLDPDUs received and then discarded due to insufficient memory space, missing or out-of-sequence attributes, or any other reason.
- **Neighbor Ageouts** – A count of the times that a neighbor's information has been deleted from the LLDP remote systems MIB because the remote TTL timer has expired.

Web – Click LLDP, Device Statistics Details.



LLDP Device Statistics Detail

Interface ● Port 1 ○ Trunk

Frames Discarded	0
Frames Invalid	0
Frames Received	114
Frames Sent	114
TLVs Unrecognized	0
TLVs Discarded	0
Neighbor Ageouts	0

Figure 12-10 LLDP Device Statistics Details

CLI – This example displays detailed LLDP statistics for an LLDP-enabled remote device attached to a specific port this switch.

```
switch#show lldp info statistics detail ethernet 1/1                 32-18

 LLDP Port Statistics Detail

  PortName            : Eth 1/1
  Frames Discarded    : 0
  Frames Invalid      : 0
  Frames Received     : 12
  Frames Sent         : 13
  TLVs Unrecognized : 0
  TLVs Discarded      : 0
  Neighbor Ageouts    : 0

switch#
```

Chapter 13: Class of Service

Class of Service (CoS) allows you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, and configure the mapping of frame priority tags to the switch's priority queues.

Layer 2 Queue Settings

Setting the Default Priority for Interfaces

You can specify the default port priority for each interface on the switch. All untagged packets entering the switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

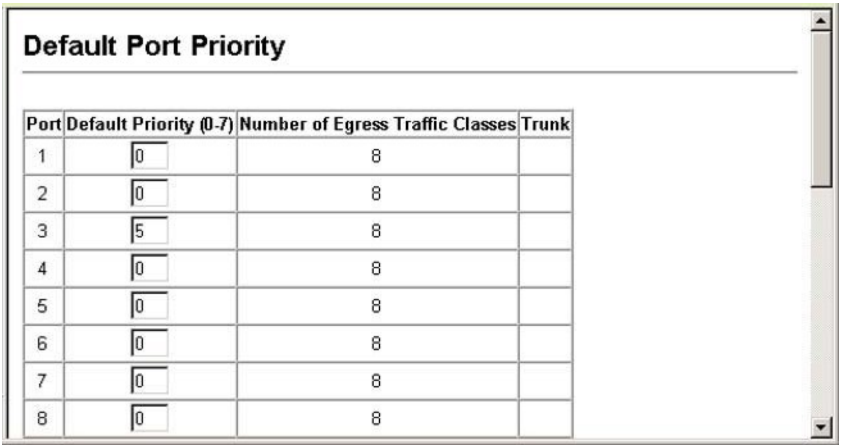
- This switch provides eight priority queues for each port. It uses Weighted Round Robin to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority**[15] – The priority that is assigned to untagged frames received on the specified interface. (Range: 0 - 7, Default: 0)
- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

[15] CLI displays this information as "Priority for untagged traffic."

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.



Default Port Priority

Port	Default Priority (0-7)	Number of Egress Traffic Classes	Trunk
1	0	8	
2	0	8	
3	5	8	
4	0	8	
5	0	8	
6	0	8	
7	0	8	
8	0	8	

Figure 13-1   Default Port Priority

CLI – This example assigns a default priority of 5 to port 3.

```
Console(config)#interface ethernet 1/3                               27-1
Console(config-if)#switchport priority default 5                     35-3
Console(config-if)#end
Console#show interfaces switchport ethernet 1/3                     27-11
Information of Eth 1/3
 Broadcast threshold:             Enabled, 500 packets/second
 LACP status:                    Disabled
 Ingress rate limit:              Disable, 1000M bits per second
 Egress rate limit:               Disable, 1000M bits per second
 VLAN membership mode:           Hybrid
 Ingress rule:                   Disabled
 Acceptable frame type:          All frames
 Native VLAN:                   1
 Priority for untagged traffic: 5
 GVRP status:                    Disabled
 Allowed VLAN:                      1(u),
 Forbidden VLAN:
Console#
```

Mapping CoS Values to Egress Queues

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 13-1 Mapping CoS Values to Egress Queues

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Table 13-2 CoS Priority Levels

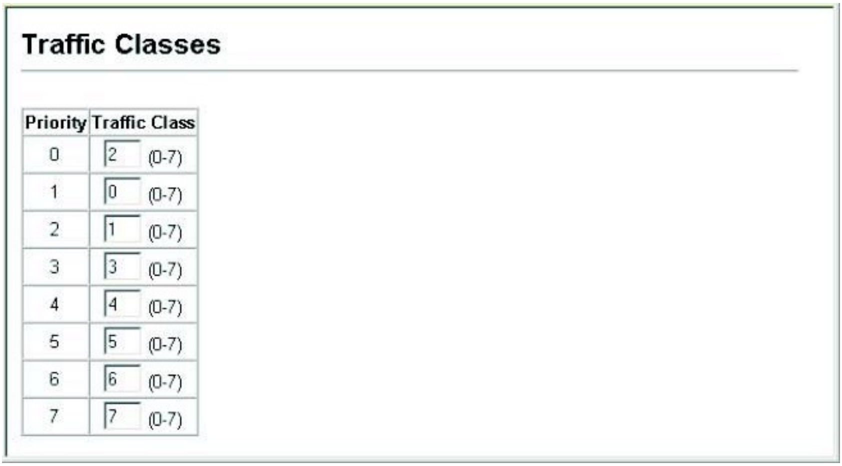
Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class**[16] – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

[16] CLI shows Queue ID.

Web – Click Priority, Traffic Classes. Assign priorities to the traffic classes (i.e., output queues), then click Apply.



Traffic Classes

Priority	Traffic Class
0	2 (0-7)
1	0 (0-7)
2	1 (0-7)
3	3 (0-7)
4	4 (0-7)
5	5 (0-7)
6	6 (0-7)
7	7 (0-7)

Figure 13-2 Traffic Classes

CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```
Console(config)#interface ethernet 1/1                                   27-1
Console(config)#queue cos-map 0 0                                        35-4
Console(config)#queue cos-map 1 1
Console(config)#queue cos-map 2 2
Console(config)#exit
Console#show queue cos-map                                               35-6
Information of Eth 1/1
 CoS Value:        0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Information of Eth 1/2
 CoS Value:        0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
:
```

* Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

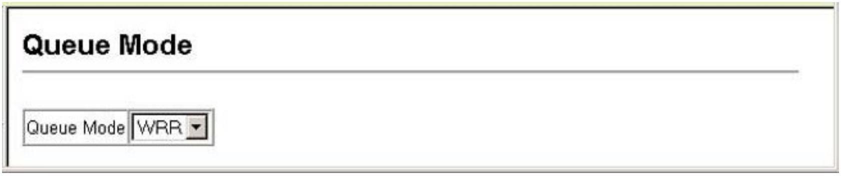
Selecting the Queue Mode

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Command Attributes

- **WRR** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively. (This is the default selection.)
- **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.

Web – Click Priority, Queue Mode. Select Strict or WRR, then click Apply.



Queue Mode

Queue Mode: WRR

Figure 13-3 Queue Mode

CLI – The following sets the queue mode to strict priority service mode.

```
Console(config)#queue mode strict                                      35-2
Console(config)#exit
Console#show queue mode                                                35-5

Queue mode: strict
Console#
```

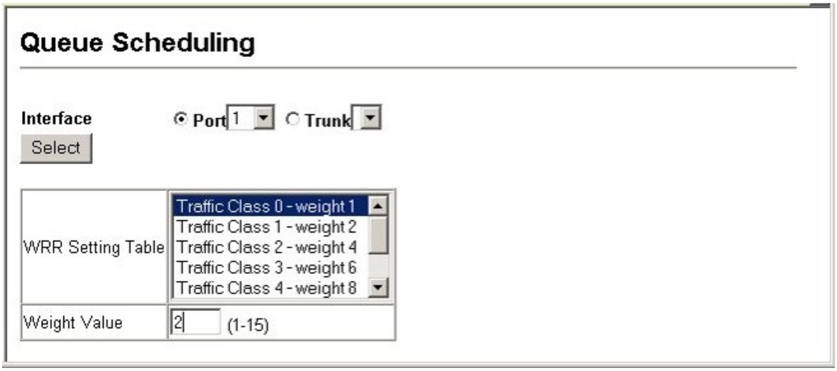
Setting the Service Weight for Traffic Classes

This switch uses the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in “Mapping CoS Values to Egress Queues” on page 3, the traffic classes are mapped to one of the eight egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table**[17] – Displays a list of weights for each traffic class (i.e., queue).
- **Weight Value** – Set a new weight for the selected traffic class. (Range: 1-15)

Web – Click Priority, Queue Scheduling. Select the interface, highlight a traffic class (i.e., output queue), enter a weight, then click Apply.



Queue Scheduling

Interface ● Port 1 ○ Trunk

WRR Setting Table	Traffic Class 0 - weight 1 Traffic Class 1 - weight 2 Traffic Class 2 - weight 4 Traffic Class 3 - weight 6 Traffic Class 4 - weight 8
Weight Value	2 (1-15)

Figure 13-4 Queue Scheduling

[17] CLI shows Queue ID.

CLI – The following example shows how to assign WRR weights to each of the priority queues.

```
Console(config)#queue bandwidth 1 3 5 7 9 11 13 15                      35-4
Console(config)#exit
Console#show queue bandwidth                                            35-6
Information of Eth 1/1
 Queue ID   Weight
 --------   ------
    0         1
    1         3
    2         5
    3         7
    4         9
    5         11
    6         13
    7         15
Information of Eth 1/2
 Queue ID   Weight
⋮
```

Layer 3/4 Priority Settings

Mapping Layer 3/4 Priorities to CoS Values

This switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, this switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

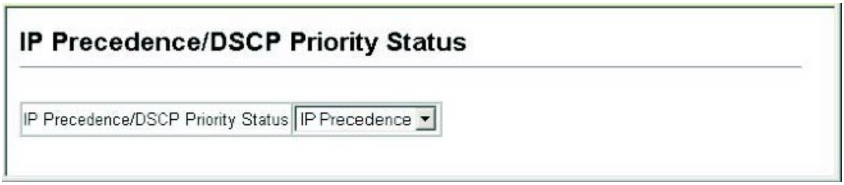
Selecting IP Precedence/DSCP Priority

The switch allows you to choose between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu, then click Apply.



IP Precedence/DSCP Priority Status

IP Precedence/DSCP Priority Status: IP Precedence

Figure 13-5 IP Precedence/DSCP Priority Status

CLI – The following example enables IP Precedence service on the switch.

```
Console(config)#map ip precedence                                    35-8
Console(config)#
```

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (i.e., Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in the following table.

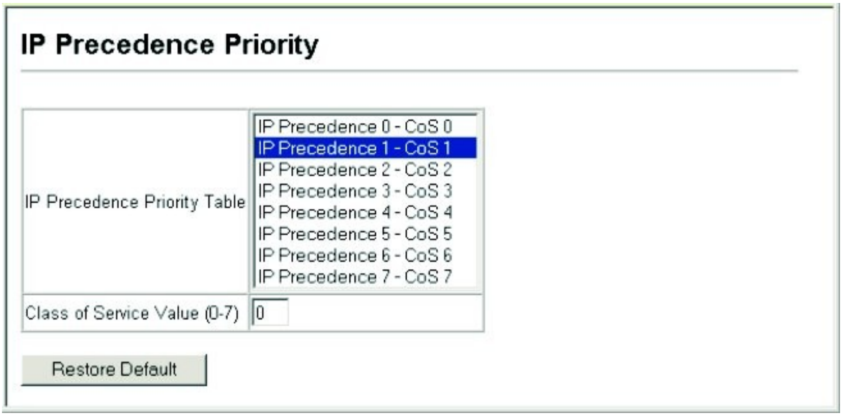
Table 13-3 Mapping IP Precedence

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “7” represent high priority.

Web – Click Priority, IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.



IP Precedence Priority

IP Precedence Priority Table	IP Precedence 0 - CoS 0 IP Precedence 1 - CoS 1 IP Precedence 2 - CoS 2 IP Precedence 3 - CoS 3 IP Precedence 4 - CoS 4 IP Precedence 5 - CoS 5 IP Precedence 6 - CoS 6 IP Precedence 7 - CoS 7
Class of Service Value (0-7)	0

Figure 13-6 IP Precedence Priority

CLI – The following example globally enables IP Precedence service on the switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```
Console(config)#map ip precedence                                        35-8
Console(config)#interface ethernet 1/1                                   27-1
Console(config-if)#map ip precedence 1 cos 0                             35-9
Console(config-if)#end
Console#show map ip precedence ethernet 1/1                             35-12
Precedence mapping status: disabled

 Port       Precedence COS
 --------- ---------- ---
  Eth 1/ 1          0   0
  Eth 1/ 1          1   0
  Eth 1/ 1          2   2
  Eth 1/ 1          3   3
  Eth 1/ 1          4   4
  Eth 1/ 1          5   5
  Eth 1/ 1          6   6
  Eth 1/ 1          7   7
Console#
```

* Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 13-4 Mapping DSCP Priority

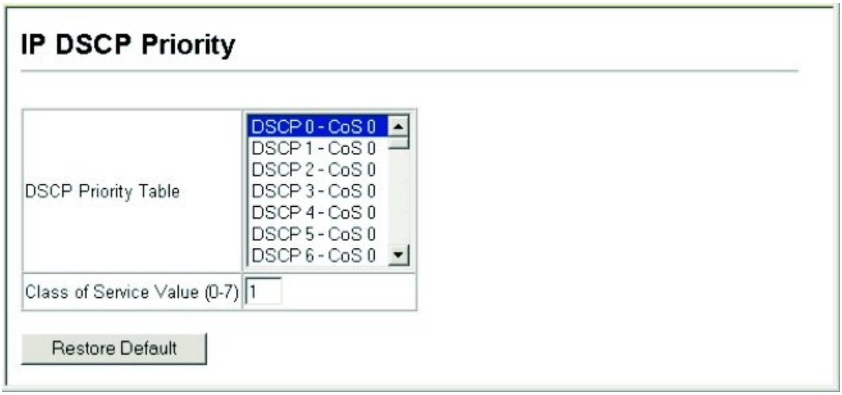
IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table –** Shows the DSCP Priority to CoS map.
- **Class of Service Value –** Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.



IP DSCP Priority

DSCP Priority Table	DSCP 0 - CoS 0 DSCP 1 - CoS 0 DSCP 2 - CoS 0 DSCP 3 - CoS 0 DSCP 4 - CoS 0 DSCP 5 - CoS 0 DSCP 6 - CoS 0
Class of Service Value (0-7)	1

Figure 13-7 IP DSCP Priority

CLI – The following example globally enables DSCP Priority service on the switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```
Console(config)#map ip dscp                                              35-10
Console(config)#interface ethernet 1/1                                    27-1
Console(config-if)#map ip dscp 1 cos 0                                   35-10
Console(config-if)#end
Console#show map ip dscp ethernet 1/1                                    35-13
DSCP mapping status: disabled

 Port       DSCP COS
 --------- ---- ---
  Eth 1/ 1     0   0
  Eth 1/ 1     1   0
  Eth 1/ 1     2   0
  Eth 1/ 1     3   0
:
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

* Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Mapping IP Port Priority

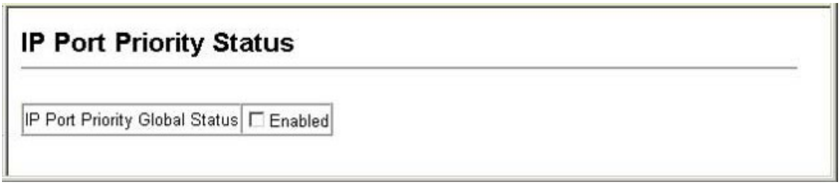
You can also map network applications to Class of Service values based on the IP port number (i.e., TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that “0” represents low priority and “7” represent high priority.

Note: Up to 8 entries can be specified.
IP Port Priority settings apply to all interfaces.

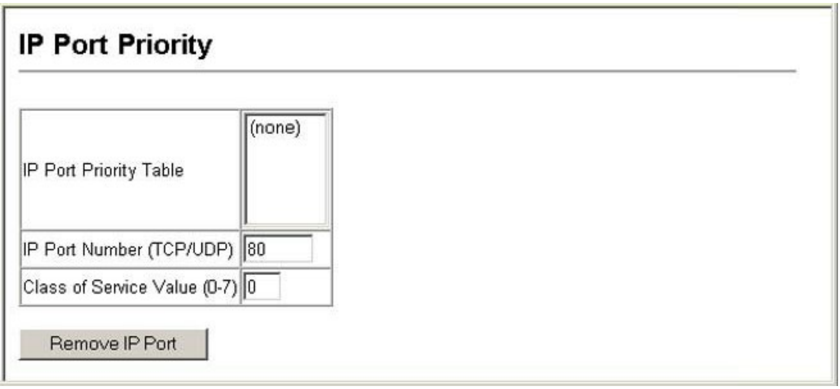
Web – Click Priority, IP Port Priority Status. Set IP Port Priority Status to Enabled.


IP Port Priority Status

IP Port Priority Global Status ☐ Enabled

Figure 13-8 IP Port Priority Status

Click Priority, IP Port Priority. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Apply.



IP Port Priority

IP Port Priority Table	(none)
IP Port Number (TCP/UDP)	80
Class of Service Value (0-7)	0

Figure 13-9 IP Port Priority

CLI – The following example globally enables IP Port Priority service on the switch, maps HTTP traffic (on port 1) to CoS value 0, and then displays the IP Port Priority settings.

```
Console(config)#map ip port                                          35-7
Console(config)#interface ethernet 1/1                               27-1
Console(config-if)#map ip port 80 cos 0                              35-8
Console(config-if)#end
Console#show map ip port ethernet 1/5                               35-11
TCP port mapping status: disabled

 Port       Port no. COS
 --------- -------- ---
  Eth 1/ 1       80   0
Console#
```

* Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the switch.

Chapter 14: Quality of Service

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Notes: **1.** You can configure up to 16 rules per Class Map. You can also include multiple classes in a Policy Map.

2. You should create a Class Map before creating a Policy Map. Otherwise, you will not be able to select a Class Map from the Policy Rule Settings screen (see page 14-6).

Configuring Quality of Service Parameters

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the “Class Map” to designate a class name for a specific category of traffic.
2. Edit the rules for each class to specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Use the “Policy Map” to designate a policy name for a specific manner in which ingress traffic will be handled.
4. Add one or more classes to the Policy Map. Assign policy rules to each class by “setting” the QoS value to be assigned to the matching traffic class. The policy rule can also be configured to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
5. Use the “Service Policy” to assign a policy map to a specific interface.

Configuring a Class Map

A class map is used for matching packets to a specified class.

Command Usage

- To configure a Class Map, follow these steps:
  - Open the Class Map page, and click Add Class.
  - When the Class Configuration page opens, fill in the “Class Name” field, and click Add.
  - When the Match Class Settings page opens, specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN, and click the Add button next to the field for the selected traffic criteria. You can specify up to 16 items to match when assigning ingress traffic to a class map.
- The class map is used with a policy map (page 14-4) to create a service policy (page 14-7) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

Command Attributes

Class Map

- **Modify Name and Description** – Configures the name and a brief description of a class map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Rules** – Opens the “Match Class Settings” page for the selected class entry. Modify the criteria used to classify ingress traffic on this page.
- **Add Class** – Opens the “Class Configuration” page. Enter a class name and description on this page, and click Add to open the “Match Class Settings” page. Enter the criteria used to classify ingress traffic on this page.
- **Remove Class** – Removes the selected class.

Class Configuration

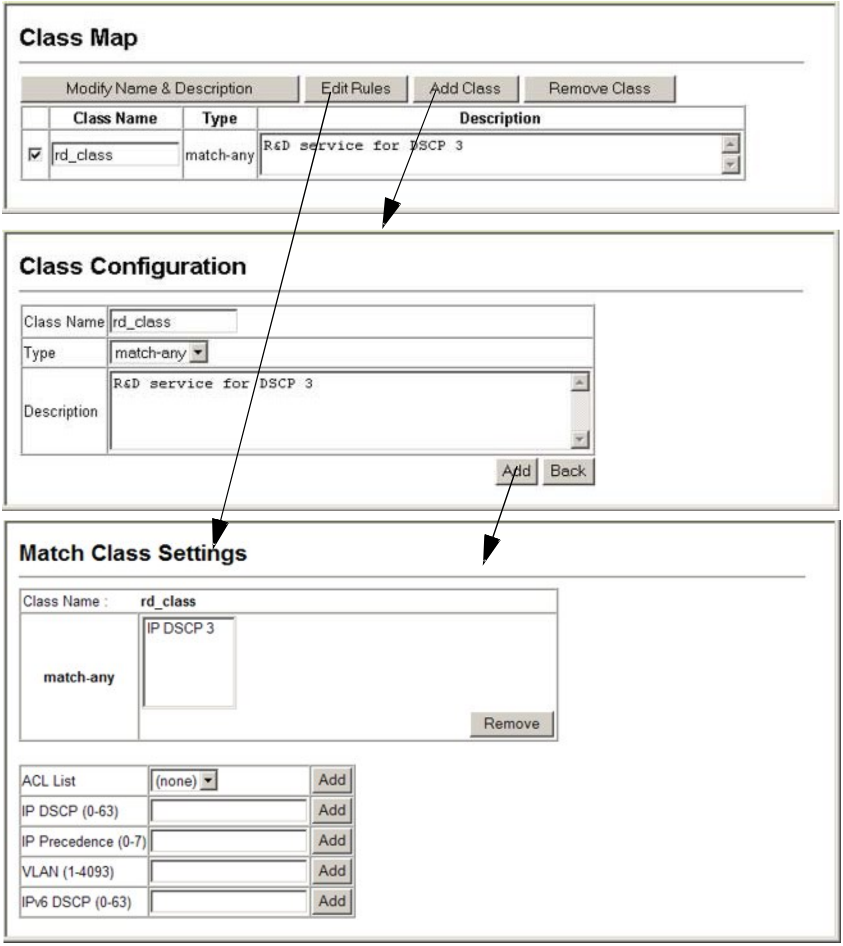
- **Class Name** – Name of the class map. (Range: 1-16 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **Description** – A brief description of a class map. (Range: 1-64 characters)
- **Add** – Adds the specified class.
- **Back** – Returns to previous page with making any changes.

Match Class Settings

- **Class Name** – List of class maps.
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **IP DSCP** – A DSCP value contained in an IPv4 packet. (Range: 0-63)

- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN** – A VLAN. (Range:1-4093)
- **IPv6 DSCP** – A DSCP value contained in an IPv6 packet. (Range: 0-63)
- **Add** – Adds specified criteria to the class. Up to 16 items are permitted per class.
- **Remove** – Deletes the selected criteria from the class.

Web – Click QoS, DiffServ, then click Add Class to create a new class, or Edit Rules to change the rules of an existing class.



Class Map

	Class Name	Type	Description
☑	rd_class	match-any	R&D service for DSCP 3

Class Configuration

Class Name	rd_class
Type	match-any
Description	R&D service for DSCP 3

Match Class Settings

Class Name :	rd_class
match-any	IP DSCP 3

ACL List	(none)	Add
IP DSCP (0-63)		Add
IP Precedence (0-7)		Add
VLAN (1-4093)		Add
IPv6 DSCP (0-63)		Add

Figure 14-1 Configuring Class Maps

CLI - This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd_class match-any                              36-2
Console(config-cmap)#match ip dscp 3                                      36-3
Console(config-cmap)#
```

Creating QoS Policies

This function creates a policy map that can be attached to multiple interfaces.

Command Usage

- To configure a Policy Map, follow these steps:
  - Create a Class Map as described on page 14-2.
  - Open the Policy Map page, and click Add Policy.
  - When the Policy Configuration page opens, fill in the “Policy Name” field, and click Add.
  - When the Policy Rule Settings page opens, select a class name from the scroll-down list (Class Name field). Configure a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed field). Then finally click Add to register the new policy.
- A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings (page 14-7). You can configure up to 64 policers (i.e., meters or class maps) for each of the following access list types: MAC ACL, IP ACL (including Standard ACL and Extended ACL), IPv6 Standard ACL, and IPv6 Extended ACL. This limitation applies to each switch chip (IC40240-10G: ports 1-26, IC40480-10G: ports 1-25, ports 26-50). Also, note that the maximum number of classes that can be applied to a policy map is 16.

  Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the “Burst” field, and the average rate tokens are removed from the bucket is by specified by the “Rate” option.
- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 14-7) to take effect.

Command Attributes

Policy Map

- **Modify Name and Description** – Configures the name and a brief description of a policy map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Classes** – Opens the “Policy Rule Settings” page for the selected class entry. Modify the criteria used to service ingress traffic on this page.

- **Add Policy** – Opens the “Policy Configuration” page. Enter a policy name and description on this page, and click Add to open the “Policy Rule Settings” page. Enter the criteria used to service ingress traffic on this page.
- **Remove Policy** – Deletes a specified policy.

Policy Configuration

- **Policy Name** — Name of policy map. (Range: 1-16 characters)
- **Description** – A brief description of a policy map. (Range: 1-64 characters)
- **Add** – Adds the specified policy.
- **Back** – Returns to previous page with making any changes.

Policy Rule Settings

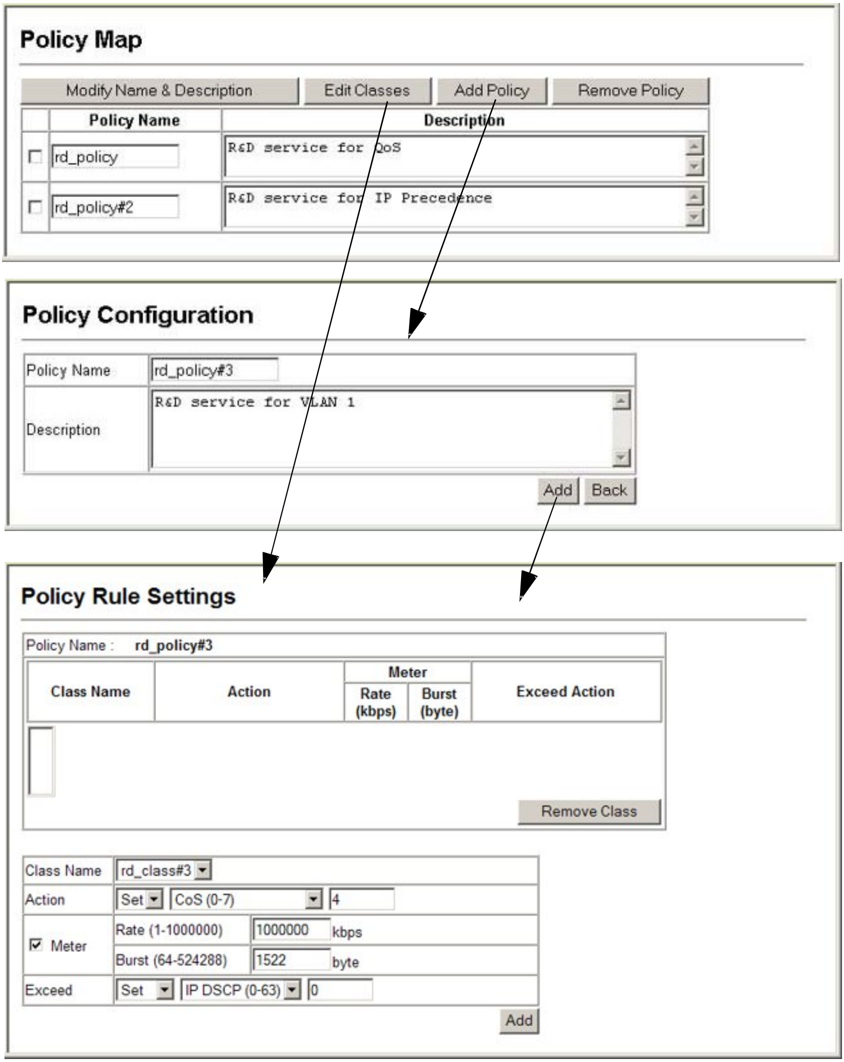
- Class Settings -

- **Class Name** – Name of class map.
- **Action** – Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 14-2).
- **Meter** – The maximum throughput and burst rate.
  - **Rate (kbps)** – Rate in kilobits per second.
  - **Burst (byte)** – Burst in bytes.
- **Exceed Action** – Specifies whether the traffic that exceeds the specified rate will be dropped or the DSCP service level will be reduced.
- **Remove Class** – Deletes a class.

- Policy Options -

- **Class Name** – Name of class map.
- **Action** – Configures the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 14-2). (Range - CoS: 0-7, DSCP: 0-63, IP Precedence: 0-7,
  IPv6 DSCP: 0-63)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
  - **Rate (kbps)** – Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
  - **Burst (byte)** – Burst in bytes. (Range: 64-524288)
- **Exceed** – Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.
  - **Set** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
  - **Drop** – Drops out of conformance traffic.
- **Add** – Adds the specified criteria to the policy map.

Web – Click QoS, DiffServ, Policy Map to display the list of existing policy maps. To add a new policy map click Add Policy. To configure the policy rule settings click Edit Classes.



Policy Map

	Policy Name	Description
□	rd_policy	R&D service for QoS
□	rd_policy#2	R&D service for IP Precedence

Policy Configuration

Policy Name	rd_policy#3
Description	R&D service for VLAN 1

Policy Rule Settings

Policy Name : rd_policy#3

Class Name	Action	Meter		Exceed Action
		Rate (kbps)	Burst (byte)	

Class Name	rd_class#3		
Action	Set	CoS (0-7)	4
☑ Meter	Rate (1-1000000)	1000000	kbps
	Burst (64-524288)	1522	byte
Exceed	Set	IP DSCP (0-63)	0

Figure 14-2 Configuring Policy Maps

CLI – This example creates a policy map called “rd-policy,” sets the average bandwidth the 1 Mbps, the burst rate to 1522 bps, and the response to reduce the DSCP value for violating packets to 0.

```
Console(config)#policy-map rd_policy#3                                  36-5
Console(config-pmap)#class rd_class#3                                   36-5
Console(config-pmap-c)#set ip dscp 4                                    36-6
Console(config-pmap-c)#police 100000 1522 exceed-action
 set ip dscp 0                                                          36-7
Console(config-pmap-c)#
```

Attaching a Policy Map to Ingress Queues

This function binds a policy map to the ingress queue of a particular interface.

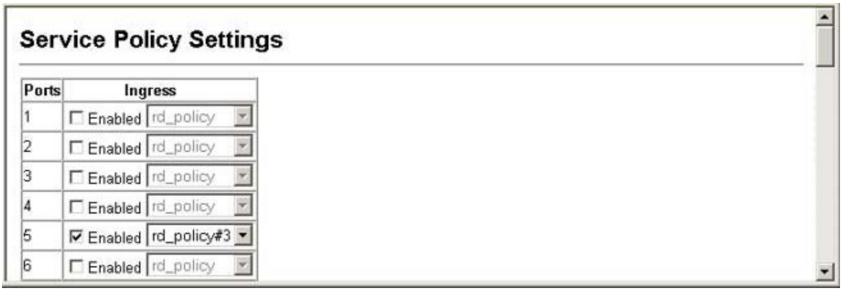
Command Usage

- You must first define a class map, then define a policy map, and finally bind the service policy to the required interface.
- You can only bind one policy map to an interface.
- The current firmware does not allow you to bind a policy map to an egress queue.

Command Attributes

- **Ports** – Specifies a port.
- **Ingress** – Applies the rule to ingress traffic.
- **Enabled** – Check this to enable a policy map on the specified port.
- Policy Map – Select the appropriate policy map from the scroll-down box.

Web – Click QoS, DiffServ, Service Policy Settings. Check Enabled and choose a Policy Map for a port from the scroll-down box, then click Apply.



Service Policy Settings

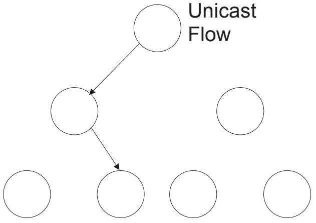
Ports	Ingress	
1	□ Enabled	rd_policy
2	□ Enabled	rd_policy
3	□ Enabled	rd_policy
4	□ Enabled	rd_policy
5	☑ Enabled	rd_policy#3
6	□ Enabled	rd_policy

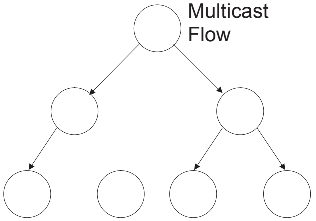
Figure 14-3 Service Policy Settings

CLI - This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/5                                  27-1
Console(config-if)#service-policy input rd_policy#3                     36-8
Console(config-if)#
```

Chapter 15: Multicast Filtering





Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/ router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts

This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query (page 15-3) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

When using IGMPv3 snooping, service requests from IGMP Version 1, 2 or 3 hosts are all forwarded to the upstream router as IGMPv3 reports. The primary enhancement provided by IGMPv3 snooping is in keeping track of information about the specific multicast sources which downstream IGMPv3 hosts have requested or refused. The switch maintains information about both multicast groups and channels, where a group indicates a multicast flow for which the hosts have not requested a specific source (the only option for IGMPv1 and v2 hosts unless statically configured on the switch), and a channel indicates a flow for which the hosts have requested service from a specific source.

Only IGMPv3 hosts can request service from a specific multicast source. When downstream hosts request service from a specific source for a multicast service, these sources are all placed in the Include list, and traffic is forwarded to the hosts from each of these sources. IGMPv3 hosts may also request that service be forwarded from all sources except for those specified. In this case, traffic is filtered from sources in the Exclude list, and forwarded from all other available sources.

Notes:

1. When the switch is configured to use IGMPv3 snooping, the snooping version may be downgraded to version 2 or version 1, depending on the version of the IGMP query packets detected on each VLAN.

2. IGMP snooping will not function unless a multicast router port is enabled on the switch. This can be accomplished in one of two ways. A static router port can be manually configured (see “Specifying Static Interfaces for a Multicast Router” on page 15-7). Using this method, the router port is never timed out, and will continue to function until explicitly removed. The other method relies on the switch to dynamically create multicast routing ports whenever multicast routing protocol packets or IGMP query packets are detected on a port.

3. A maximum of up to 255 multicast entries can be maintained for IGMP snooping, and 255 entries for Multicast Routing, when both of these features are enabled. If the table’s capacity is exceeded, the IGMPv3 snooping will not support multicast source filtering, but will forward multicast traffic from all relevant sources to the requesting hosts.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, you can manually designate a known IGMP querier (i.e., a multicast router/switch) connected over the network to an interface on your switch (page 15-7). This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the switch.

Static IGMP Host Interface – For multicast applications that you need to control more carefully, you can manually assign a multicast service to specific interfaces on the switch (page 15-9).

Configuring IGMP Snooping and Query Parameters

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

Note: Unknown multicast traffic is flooded to all ports in the VLAN for several seconds when first received. If a multicast router port exists on the VLAN, the traffic will be filtered by subjecting it to IGMP snooping. If no router port exists on the VLAN or the multicast filtering table is already full, the switch will continue flooding the traffic into the VLAN.

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

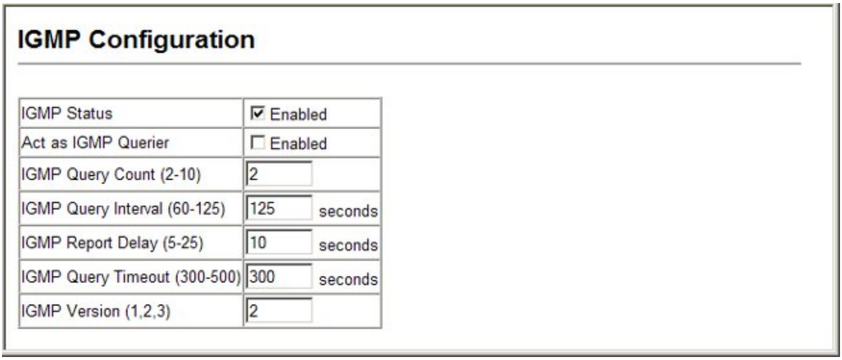
- **IGMP Status** — When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)
- **Act as IGMP Querier** — When enabled, the switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. This feature is not supported for IGMPv3 snooping. (Default: Disabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 5-25 seconds, Default: 10)

- **IGMP Query Timeout** — The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. (Range: 1-3; Default: 2)

Notes: **1.** All systems on the subnet must support the same version.

2. Some attributes are only enabled for IGMPv2, including IGMP Report Delay and IGMP Query Timeout.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown below.)



IGMP Configuration

IGMP Status	☑ Enabled
Act as IGMP Querier	□ Enabled
IGMP Query Count (2-10)	2
IGMP Query Interval (60-125)	125 seconds
IGMP Report Delay (5-25)	10 seconds
IGMP Query Timeout (300-500)	300 seconds
IGMP Version (1,2,3)	2

Figure 15-1 IGMP Configuration

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```
Console(config)#ip igmp snooping                                    37-1
Console(config)#ip igmp snooping querier                            37-5
Console(config)#ip igmp snooping query-count 10                     37-6
Console(config)#ip igmp snooping query-interval 100                 37-7
Console(config)#ip igmp snooping query-max-response-time 20         37-7
Console(config)#ip igmp snooping router-port-expire-time 300        37-8
Console(config)#ip igmp snooping version 2                          37-2
Console(config)#exit
Console#show ip igmp snooping                                       37-4
 Service Status:            Enabled
 Querier Status:            Enabled
 Query Count:               10
 Query Interval:            100 sec
 Query Max Response Time: 20 sec
 Router Port Expire Time: 300 sec
 Immediate Leave Processing: Disabled on all VLAN
 IGMP Snooping Version:     Version 2
Console#
```

Enabling IGMP Immediate Leave

The switch can be configured to immediately delete a member port of a multicast service if a leave packet is received at that port and the immediate-leave function is enabled for the parent VLAN. This allows the switch to remove a port from the multicast forwarding table without first having to send an IGMP group-specific query to that interface.

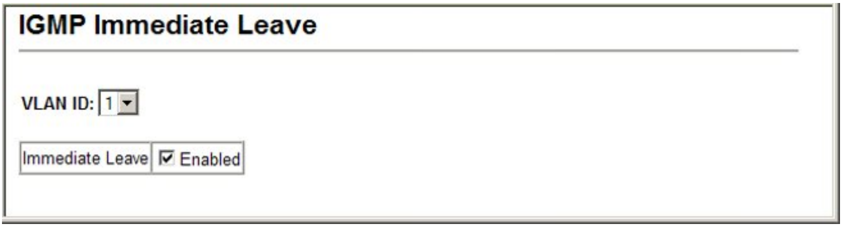
Command Usage

- If immediate leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period. Note that the timeout period is determined by the IGMP Query Report Delay (see “Configuring IGMP Snooping and Query Parameters” on page 15-3).
- If immediate leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- Immediate leave is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.
- Immediate leave does not apply to a port if the switch has learned that a multicast router is attached to it.
- Immediate leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests.

Command Attributes

- **VLAN ID** – VLAN Identifier. (Range: 1-4093).
- **Immediate Leave** – Sets the status for immediate leave on the specified VLAN. (Default: Disabled)

Web – Click IGMP Snooping, IGMP Immediate Leave. Select the VLAN interface to configure, set the status for immediate leave, and click Apply.



IGMP Immediate Leave

VLAN ID: 1

Immediate Leave ☑ Enabled

Figure 15-1 IGMP Immediate Leave

CLI – This example enables IGMP immediate leave for VLAN 1 and then displays the current IGMP snooping status.

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp snooping immediate-leave                 37-3
Console(config-if)#end
Console#show ip igmp snooping                                       37-4
 Service Status:            Enabled
 Querier Status:            Disabled
 Leave proxy status:        Enabled
 Query Count:              2
 Query Interval:            125 sec
 Query Max Response Time: 10 sec
 Router Port Expire Time: 300 sec
 Immediate Leave Processing: Enabled on VLAN      1,
 IGMP Snooping Version:     Version 2
Console#
```

Displaying Interfaces Attached to a Multicast Router

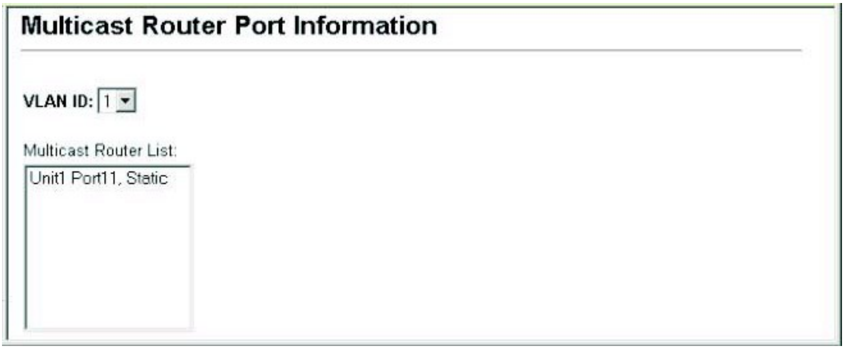
Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the switch or statically assigned to an interface on the switch.

You can use the Multicast Router Port Information page to display the ports on this switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4093).
- **Multicast Router List** – Multicast routers dynamically discovered by this switch or those that are statically assigned to an interface on this switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.


Multicast Router Port Information

VLAN ID: 1

Multicast Router List:

Unit1 Port11, Static

Figure 15-2 Multicast Router Port Information

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1                          37-10
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1            Eth 1/11 Static
Console#
```

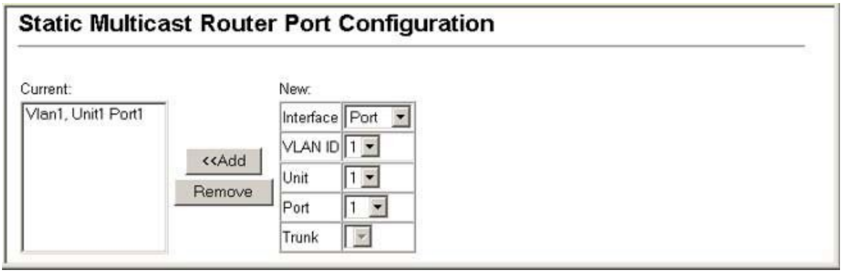
Specifying Static Interfaces for a Multicast Router

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on your switch, you can manually configure the interface (and a specified VLAN) to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the switch.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Unit** – Stack unit. (Range: 1-8)
- **Port** or **Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After you have finished adding interfaces to the list, click Apply.



Static Multicast Router Port Configuration

Current:

Vlan1, Unit1 Port1

New:

Interface	Port
VLAN ID	1
Unit	1
Port	1
Trunk	

Figure 15-3 Static Multicast Router Port Configuration

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11          37-9
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1                          37-10
 VLAN M'cast Router Port Type
 ---- ----------------- -------
    1            Eth 1/11  Static
Console#
```

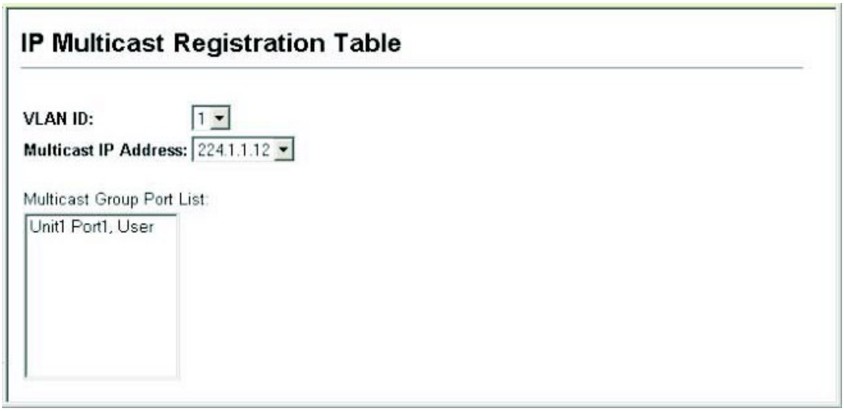
Displaying Port Members of Multicast Services

You can display the port members associated with a specified VLAN and multicast service.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members. (Range: 1-4093)
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The switch will display all the interfaces that are propagating this multicast service.



IP Multicast Registration Table

VLAN ID: 1

Multicast IP Address: 224.1.1.12

Multicast Group Port List:

Unit1 Port1, User

Figure 15-4 IP Multicast Registration Table

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

```
Console#show mac-address-table multicast vlan 1                      37-4
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1      224.1.1.12       Eth1/12     USER
    1       224.1.2.3       Eth1/12     IGMP
Console#
```

Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in “Configuring IGMP Snooping and Query Parameters” on page 15-3. For certain applications that require tighter control, you may need to statically configure a multicast service on the switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attribute

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router/switch. (Range: 1-4093)
- **Multicast IP** – The IP address for a specific multicast service
- **Unit** – Stack unit. (Range: 1-8)
- **Port** or **Trunk** – Specifies the interface attached to a multicast router/switch.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (via an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After you have completed adding ports to the member list, click Apply.

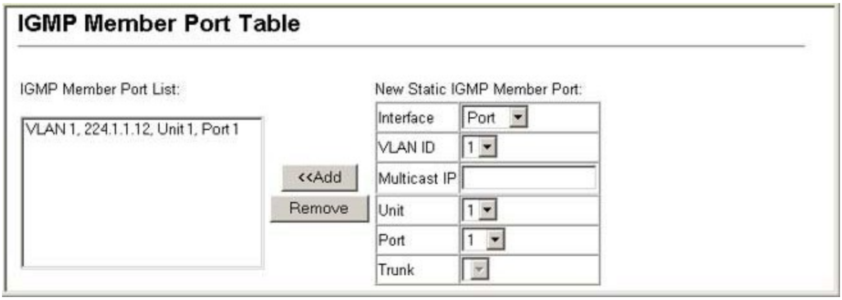


Figure 15-5 IGMP Member Port Table

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
 ethernet 1/12                                                37-2
Console(config)#exit
Console#show mac-address-table multicast vlan 1               37-4
 VLAN M'cast IP addr. Member ports Type
 ---- --------------- ------------ -------
    1       224.1.1.12       Eth1/12     USER
    1         224.1.2.3      Eth1/12     IGMP
```

Chapter 16: Domain Name Service

The Domain Naming System (DNS) service on this switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates this switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the switch, and waiting for a response.

You can manually configure entries in the DNS table used for mapping domain names to IP addresses, configure default domain names, or specify one or more name servers to use for domain name to address translation.

Configuring General DNS Service Parameters

Command Usage

- To enable DNS service on this switch, first configure one or more name servers, and then enable domain lookup status.
- To append domain names to incomplete host names received from a DNS client (i.e., not formatted with dotted notation), you can specify a default domain name or a list of domain names to be tried in sequential order.
- If there is no domain list, the default domain name is used. If there is a domain list, the system will search it for a corresponding entry. If none is found, the default domain name is used.
- When an incomplete host name is received by the DNS service on this switch and a domain name list has been specified, the switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- Note that if all name servers are deleted, DNS will automatically be disabled.

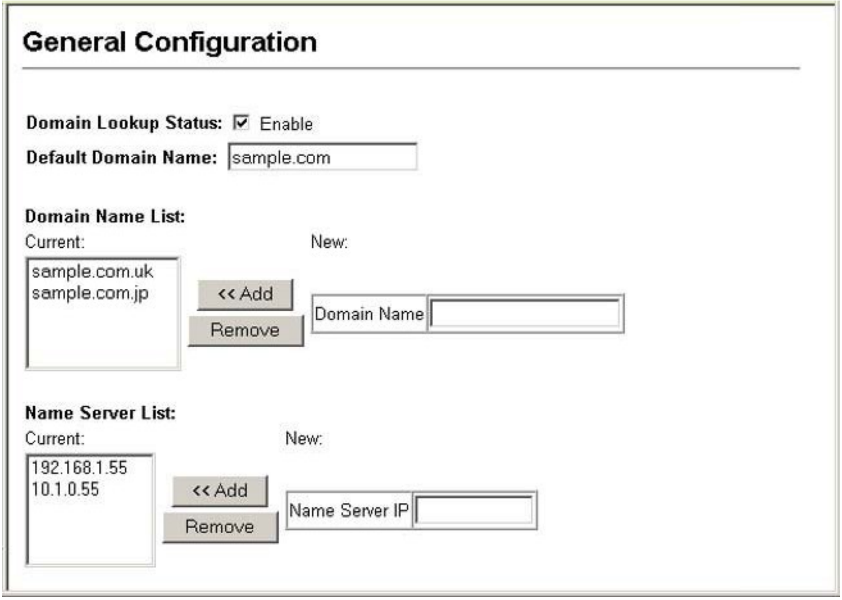
Command Attributes

- **Domain Lookup Status** – Enables DNS host name-to-address translation.
- **Default Domain Name**[18] – Defines the default domain name appended to incomplete host names. (Range: 1-127 alphanumeric characters)
- **Domain Name List[18]** – Defines a list of domain names that can be appended to incomplete host names. (Range: 1-127 alphanumeric characters; 1-3 names)
- **Name Server List** – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

Note: When specifying names, do not include the initial dot that separates the host name from the domain name.

[18] Do not include the initial dot that separates the host name from the domain name.

Web – Select DNS, General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use to use for address resolution, enable domain lookup status, and click Apply.



General Configuration

Domain Lookup Status: ☑ Enable

Default Domain Name: sample.com

Domain Name List:

Current:

sample.com.uk
sample.com.jp

Name Server List:

Current:

192.168.1.55
10.1.0.55

Figure 16-1 DNS General Configuration

CLI - This example sets a default domain name and a domain list. However, remember that if a domain list is specified, the default domain name is not used.

```
Console(config)#ip domain-name sample.com                            38-3
Console(config)#ip domain-list sample.com.uk                         38-3
Console(config)#ip domain-list sample.com.jp
Console(config)#ip name-server 192.168.1.55 10.1.0.55                38-4
Console(config)#ip domain-lookup                                     38-5
Console#show dns                                                     38-7
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.uk
    .sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Configuring Static DNS Host to Address Entries

You can manually configure static entries in the DNS table that are used to map domain names to IP addresses.

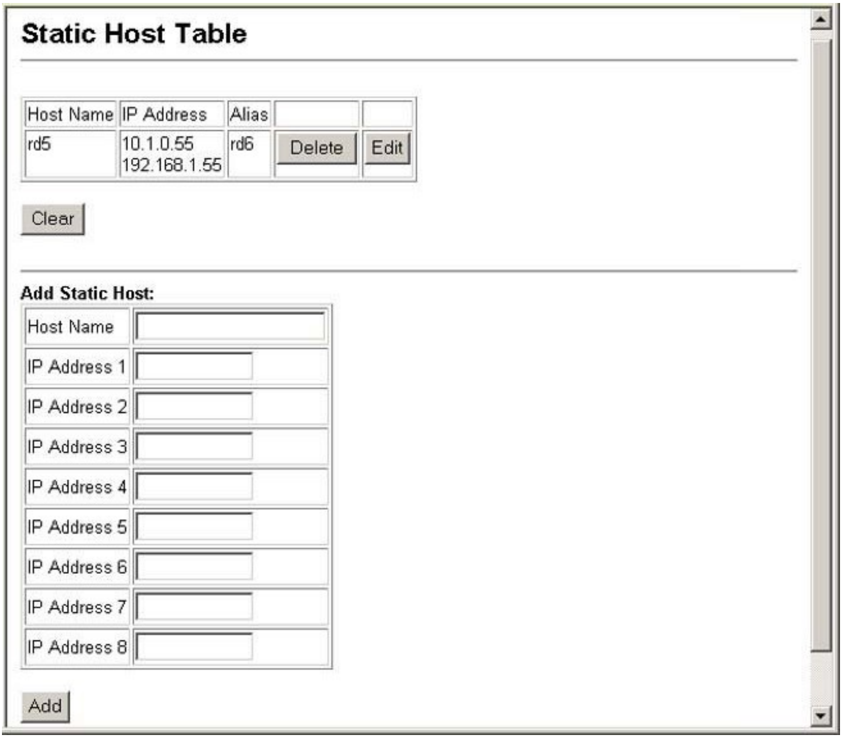
Command Usage

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.
- Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name in the static table or via information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Field Attributes

- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-127 characters)
- **IP Address** – Internet address(es) associated with a host name. (Range: 1-8 addresses)
- **Alias** – Displays the host names that are mapped to the same address(es) as a previously configured entry.

Web – Select DNS, Static Host Table. Enter a host name and one or more corresponding addresses, then click Apply.



Static Host Table

Host Name	IP Address	Alias		
rd5	10.1.0.55 192.168.1.55	rd6	Delete	Edit

Add Static Host:

Host Name	
IP Address 1	
IP Address 2	
IP Address 3	
IP Address 4	
IP Address 5	
IP Address 6	
IP Address 7	
IP Address 8	

Figure 16-2 DNS Static Host Table

CLI - This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55                    38-1
Console(config)#ip host rd6 10.1.0.55
Console#show hosts                                                    38-6

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 rd6
Console#
```

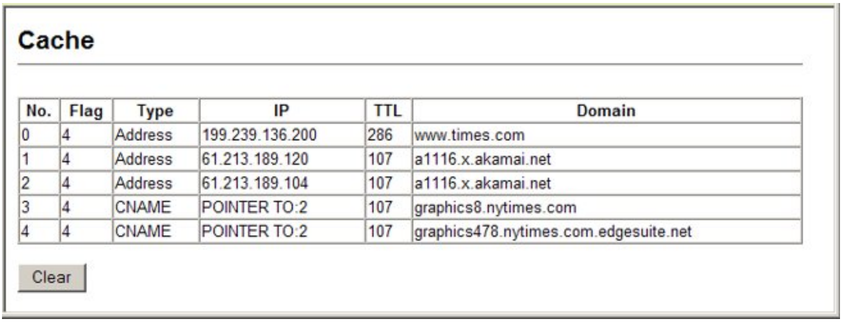
Displaying the DNS Cache

You can display entries in the DNS cache that have been learned via the designated name servers.

Field Attributes

- **No** – The entry number for each resource record.
- **Flag** – The flag is always “4” indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
- **Type** – This field includes ADDRESS which specifies the host address for the owner, and CNAME which specifies an alias.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

Web – Select DNS, Cache.



No.	Flag	Type	IP	TTL	Domain
0	4	Address	199.239.136.200	286	www.times.com
1	4	Address	61.213.189.120	107	a1116.x.akamai.net
2	4	Address	61.213.189.104	107	a1116.x.akamai.net
3	4	CNAME	POINTER TO:2	107	graphics8.nytimes.com
4	4	CNAME	POINTER TO:2	107	graphics478.nytimes.com.edgesuite.net

Figure 16-3 DNS Cache

CLI - This example displays all the resource records learned from the designated name servers.

```
Console#show  dns  cache                                                 38-7
NO       FLAG     TYPE     DOMAIN                               TTL      IP
0        4        Address www.times.com                          198      199.239.136.200
1        4        Address a1116.x.akamai.net                    19       61.213.189.120
2        4        Address a1116.x.akamai.net                    19       61.213.189.104
3        4        CNAME    graphics8.nytimes.com                19       POINTER TO:2
4        4        CNAME     graphics478.nytimes.com.edgesui 19         POINTER TO:2
Console#
```

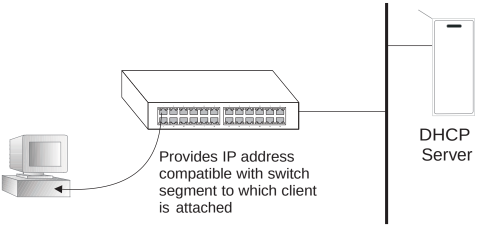
Chapter 17: Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, you can relay DHCP client requests to a DHCP server on another subnet, or configure the DHCP server on this switch to support that subnet.

When configuring the DHCP server on this switch, you can configure an address pool for each unique IP interface, or manually assign a static IP address to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

Configuring DHCP Relay Service

This switch supports DHCP relay service for attached host devices. If DHCP relay is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.


Provides IP address compatible with switch segment to which client is attached
DHCP Server

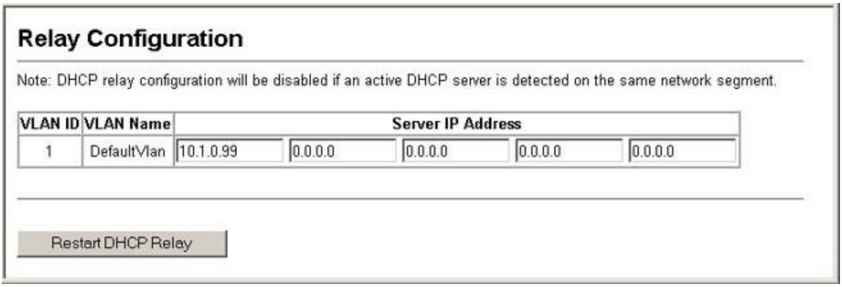
Command Usage

You must specify the IP address for at least one DHCP server. Otherwise, the switch's DHCP relay agent will not forward client requests to a DHCP server.

Command Attributes

- **VLAN ID** – ID of configured VLAN.
- **VLAN Name** – Name of the VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the switch's DHCP relay agent in order of preference.
- **Restart DHCP Relay** – Use this button to enable or re-initialize DHCP relay service.

Web – Click DHCP, Relay Configuration. Enter up to five IP addresses for any VLAN, then click Restart DHCP Relay to start the relay service.



Relay Configuration

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

VLAN ID	VLAN Name	Server IP Address				
1	DefaultVlan	10.1.0.99	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Figure 17-1 DHCP Relay Configuration

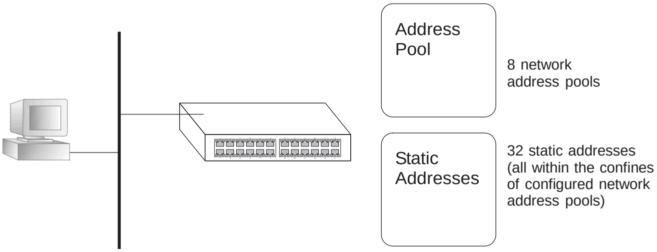
CLI – This example specifies one DHCP relay server for VLAN 1, and enables the relay service.

```
Console(config)#interface vlan 1                                 27-1
Console(config-if)#ip dhcp relay server 10.1.0.99                39-4
Console(config-if)#ip dhcp restart relay                         39-3
Console(config-if)#
```

Configuring the DHCP Server

This switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on this switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.



Address Pool
8 network address pools
Static Addresses
32 static addresses (all within the confines of configured network address pools)

Command Usage

- First configure any excluded addresses, including the address for this switch.
- Then configure address pools for the network interfaces. You can configure up to 8 network address pools. You can also manually bind an address to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. You can configure up to 32 fixed host addresses (i.e., entering one address per pool).
- If the DHCP server is running, you must disable it and then reenable it to implement any configuration changes. This can be done on the DHCP, Server, General page.

Enabling the Server, Setting Excluded Addresses

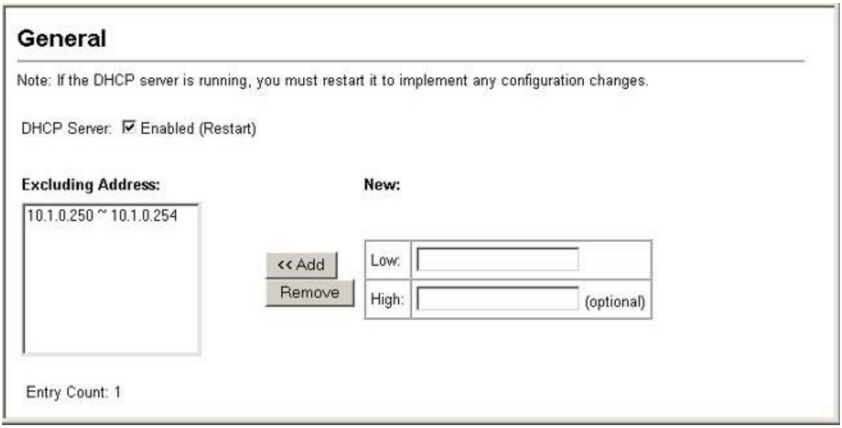
Enable the DHCP Server and specify the IP addresses that it should not be assigned to clients.

Command Attributes

- **DHCP Server** – Enables or disables the DHCP server on this switch. (Default: Disabled)
- **Excluded Addresses** – Specifies IP addresses that the DHCP server should not assign to DHCP clients. You can specify a single address or an address range.
- **New** (Excluded Addresses) – New entries for excluded addresses can be specified as a single address or an address range.

Note: Be sure you exclude the address for this switch and other key network devices.

Web – Click DHCP, Server, General. Enter a single address or an address range, and click Add.



General

Note: If the DHCP server is running, you must restart it to implement any configuration changes.

DHCP Server: ☑ Enabled (Restart)

Excluding Address:

10.1.0.250 ~ 10.1.0.254

New:

Low:

High: (optional)

Entry Count: 1

Figure 17-2 DHCP Server General Configuration

CLI – This example enables the DHCP and sets an excluded address range.

```
Console(config)#service dhcp                                             39-5
Console(config)#ip dhcp excluded-address 10.1.0.250 10.1.0.254           39-6
Console#
```

Configuring Address Pools

You must configure IP address pools for each IP interface that will provide addresses to attached clients via the DHCP server.

Command Usage

- First configure address pools for the network interfaces. Then you can manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., one address per host pool).
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- When searching for a manual binding, the switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, you must configure a hardware address for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the switch will assign an address from the first matching network pool.
- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see page 20-5). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the IP Excluded Address field on the DHCP Server General configuration page.

Command Attributes

Creating a New Address Pool

- **Pool Name** – A string or integer. (Range: 1-8 characters)
- **Type** – Shows is address pool type is Network or Host.
- **IP Address** – The IP address upon which the pool is based.
- **Mask** – Shows the network (or subnet) and the host portion of the address pool.
- **Active Pool** – The addresses provided by this pool, including those specified by the IP address and network mask, but minus those excluded on the DHCP server’s General Configuration page.

- **Configure** – Click this button to configure the corresponding address pool.

Setting the Network Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Setting the Host Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – Specifies the network mask of the client.
- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI; Default: Ethernet)
- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value.

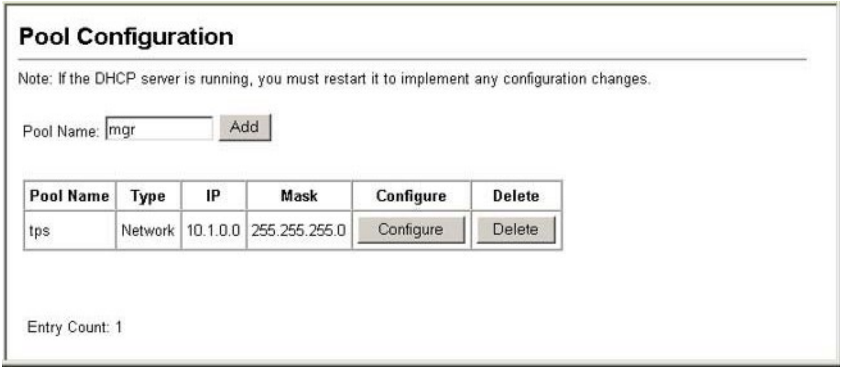
Setting the Optional Parameters

- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.
- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-128 characters)
- **Bootfile** – The default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: fixed period, Infinite; Default: 1 day)

Examples

Creating a New Address Pool

Web – Click DHCP, Server, Pool Configuration. Specify a pool name, then click Add.



Pool Configuration

Note: If the DHCP server is running, you must restart it to implement any configuration changes.

Pool Name: mgr

Pool Name	Type	IP	Mask	Configure	Delete
tps	Network	10.1.0.0	255.255.255.0	Configure	Delete

Entry Count: 1

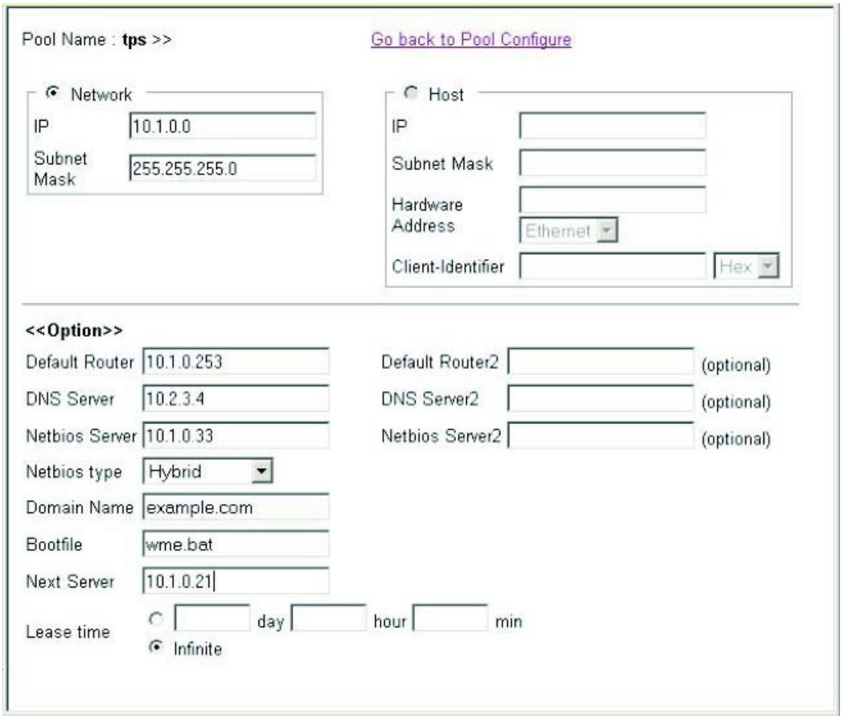
Figure 17-3 DHCP Server Pool Configuration

CLI – This example adds an address pool and enters DHCP pool configuration mode.

```
Console(config)#ip dhcp pool mgr                                    39-6
Console(config-dhcp)#
```

Configuring a Network Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for “Network.” Enter the IP address and subnet mask for the network pool. Configure the optional parameters such as gateway server and DNS server. Then click Apply.



Pool Name : **tps** >>

Go back to Pool Configure

● Network

IP: 10.1.0.0

Subnet Mask: 255.255.255.0

○ Host

IP:

Subnet Mask:

Hardware Address: Ethernet

Client-Identifier: Hex

<<Option>>

Default Router: 10.1.0.253

Default Router2: (optional)

DNS Server: 10.2.3.4

DNS Server2: (optional)

Netbios Server: 10.1.0.33

Netbios Server2: (optional)

Netbios type: Hybrid

Domain Name: example.com

Bootfile: wme.bat

Next Server: 10.1.0.21

Lease time: ○ day hour min

● Infinite

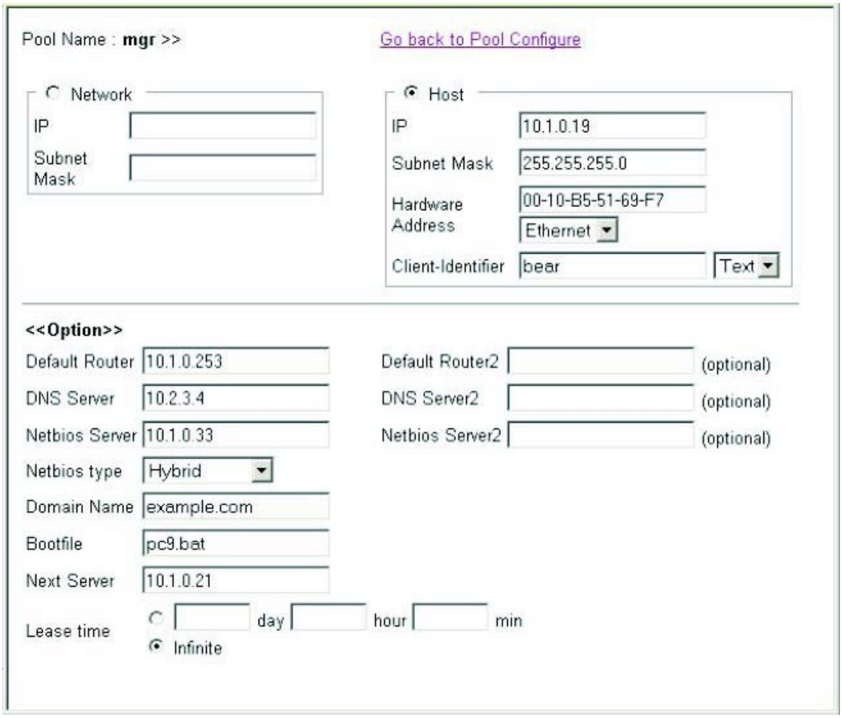
Figure 17-4 DHCP Server Pool - Network Configuration

CLI – This example configures a network address pool.

```
Console(config)#ip dhcp pool tps                                 39-6
Console(config-dhcp)#network 10.1.0.0 255.255.255.0              39-7
Console(config-dhcp)#default-router 10.1.0.253                   39-8
Console(config-dhcp)#dns-server 10.2.3.4                         39-9
Console(config-dhcp)#netbios-name-server 10.1.0.33               39-10
Console(config-dhcp)#netbios-node-type hybrid                    39-11
Console(config-dhcp)#domain-name example.com                     39-8
Console(config-dhcp)#bootfile wme.bat                            39-10
Console(config-dhcp)#next-server 10.1.0.21                       39-9
Console(config-dhcp)#lease infinite                              39-11
Console(config-dhcp)#
```

Configuring a Host Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for “Host.” Enter the IP address, subnet mask, and hardware address for the client device. Configure the optional parameters such as gateway server and DNS server. Then click Apply.



Pool Name : **mgr** >>   Go back to Pool Configure

○ Network
- IP:
- Subnet Mask:

● Host
- IP: 10.1.0.19
- Subnet Mask: 255.255.255.0
- Hardware Address: 00-10-B5-51-69-F7 Ethernet
- Client-Identifier: bear Text

<<Option>>

Default Router	10.1.0.253	Default Router2		(optional)
DNS Server	10.2.3.4	DNS Server2		(optional)
Netbios Server	10.1.0.33	Netbios Server2		(optional)
Netbios type	Hybrid			
Domain Name	example.com			
Bootfile	pc9.bat			
Next Server	10.1.0.21			

Lease time ○ day hour min
● Infinite

Figure 17-5 DHCP Server Pool - Host Configuration

CLI – This example configures a host address pool.

```
Console(config)#ip dhcp pool mgr                                       39-6
Console(config-dhcp)#host 10.1.0.19 255.255.255.0                      39-12
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet       39-14
Console(config-dhcp)#client-identifier text bear                       39-13
Console(config-dhcp)#default-router 10.1.0.253                         39-8
Console(config-dhcp)#dns-server 10.2.3.4                               39-9
Console(config-dhcp)#netbios-name-server 10.1.0.33                     39-10
Console(config-dhcp)#netbios-node-type hybrid                          39-11
Console(config-dhcp)#domain-name example.com                           39-8
Console(config-dhcp)#bootfile wme.bat                                  39-10
Console(config-dhcp)#next-server 10.1.0.21                             39-9
Console(config-dhcp)#lease infinite                                    39-11
Console(config-dhcp)#
```

Displaying Address Bindings

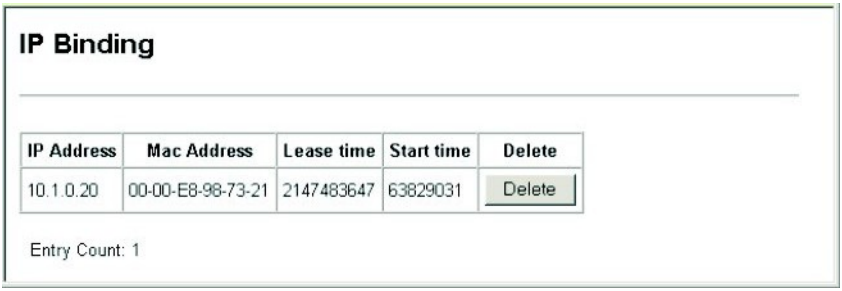
You can display the host devices which have acquired an IP address from this switch’s DHCP server.

Command Attributes

- **IP Address** – IP address assigned to host.
- **Mac Address** – MAC address of host.
- **Lease time** – Duration that this IP address can be used by the host.
- **Start time** – Time this address was assigned by the switch.
- **Delete** – Clears this binding to the host. This command is normally used after modifying the address pool, or after moving DHCP service to another device.
- **Entry Count** – Number of hosts that have been given addresses by the switch.

Note: More than one DHCP server may respond to a service request by a host. In this case, the host generally accepts the first address assigned by any DHCP server.

Web – Click DHCP, Server, IP Binding. You may use the Delete button to clear an address from the DHCP server’s database.



IP Binding

IP Address	Mac Address	Lease time	Start time	Delete
10.1.0.20	00-00-E8-98-73-21	2147483647	63829031	Delete

Entry Count: 1

Figure 17-6 DHCP Server - IP Binding

CLI – This example displays the current binding, and then clears all automatic binding.

```
Console#show ip dhcp binding                                                 39-15

     IP                   MAC          Lease Time      Start
--------------- ----------------- ------------ -----------
     10.1.0.20 00-00-e8-98-73-21            86400 Dec 25 08:01:57 2002
Console#clear ip dhcp binding *                                              39-14
Console#
```

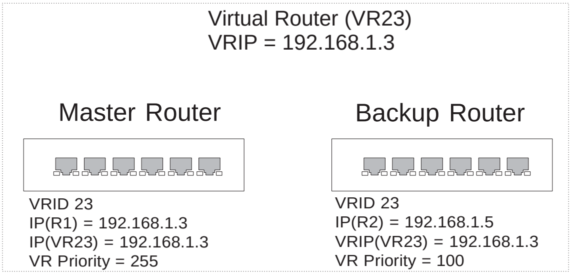
Chapter 18: Configuring Router Redundancy

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

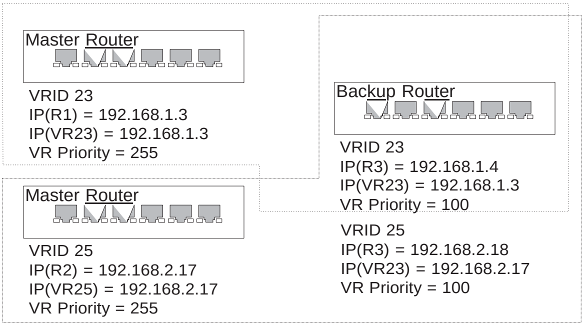
This switch supports the Virtual Router Redundancy Protocol (VRRP). VRRP allows you to specify the interface of one of the routers participating in the virtual group as the address for the master virtual router, or to configure an arbitrary address for the virtual master router. VRRP then selects the backup routers based on the specified virtual router priority.

Router redundancy can be set up in any of the following configurations. These examples use the address of one of the participating routers as the master router. When the virtual router IP address is not a real address, the master router is selected based on priority. When the priority is the same on several competing routers, then the router with the highest IP address is selected as the master.

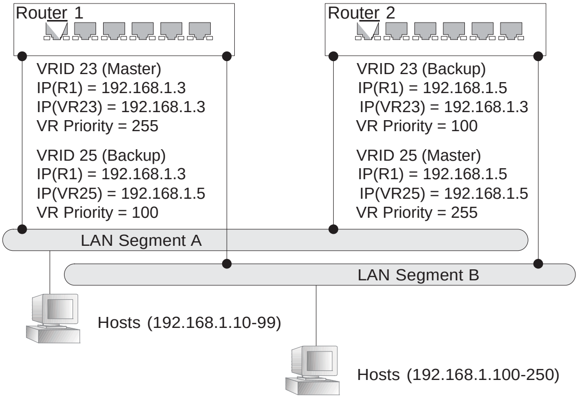
- A master virtual router with one or more backup routers.



- Several virtual master routers using the same set of backup routers.



- Several virtual master routers configured for mutual backup and load sharing. Load sharing can be accomplished by assigning a subset of addresses to different host address pools using the DHCP server. (See “Configuring Address Pools” on page 17-4.)



Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) allows you to configure a group of routers as a single virtual router. The virtual router group is configured with a single virtual IP address that can be used as the default gateway for host devices on the attached network.

Configuring VRRP Groups

To configure VRRP, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

Command Usage

Address Assignment –

- To designate a specific router as the VRRP master, the IP address assigned to the virtual router must already be configured on the router that will become the Owner of the group address. In other words, the IP address for the virtual router exists on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.
- If a virtual address is assigned to the group which does not exist on any of the group members, then the master router is selected based on priority. In cases

where the configured priority is the same on several group members, then the master router with the highest IP address is selected from this group.

- If you have multiple secondary addresses configured on the current VLAN interface, you can add any of these addresses to the virtual router group.
- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- VRRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

Virtual Router Priority –

- The Owner of the virtual IP address is automatically assigned the highest possible virtual router priority of 255. The backup router with the highest priority will become the master router if the current master fails. However, because the priority of the virtual IP address Owner is the highest, the original master router will always become the active master router when it recovers.
- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

Preempting the Acting Master –

- The virtual IP Owner has the highest priority, so no other router can preempt it, and it will always resume control as the master virtual router when it comes back on line. The preempt function only allows a backup router to take over from a master router if no router in the group is the virtual IP owner, or from another backup router that is temporarily acting as the group master. If preemption is enabled and this router has a higher priority than the current acting master when it comes on line, it will take over as the acting group master.
- You can add a delay to the preempt function to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

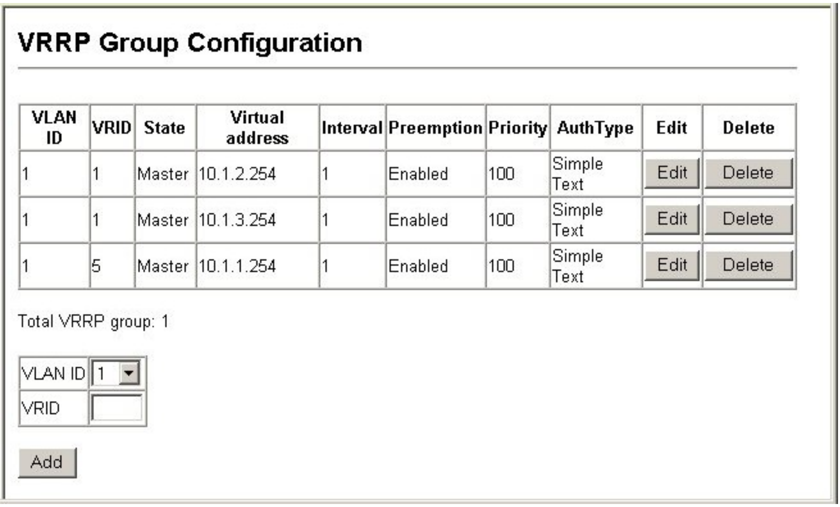
Field Attributes (VRRP Group Configuration)

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4093; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **State** – VRRP router role. (Values: Master, Backup)
- **Virtual Address** – Virtual IP address for this group.
- **Interval** – Interval (in seconds) at which the master virtual router sends advertisements communicating its state as the master.
- **Preemption** – Shows if this router is allowed to preempt the acting master.
- **Priority** – Priority of this router in the VRRP group.
- **AuthType** – Authentication mode used to verify VRRP packets from other routers.

Command Attributes (VRRP Group Configuration Detail)

- **Associated IP Table** – IP interfaces associated with this virtual router group.
- **Associated IP** – IP address of the virtual router, or secondary IP addresses assigned to the current VLAN interface that are supported by this VRRP group. If this address matches a real interface on this switch, then this interface will become the virtual master router for this VRRP group.
- **Advertisement Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master. (Range: 1-255 seconds; Default: 1 second)
  - VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
  - VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.
  - If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second.
- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router (i.e., a master router that is not the group’s address owner, or another backup router that has taken over from the previous master.) (Default: Enabled)
- **Preempt Delay** – Time to wait before issuing a claim to become the master. (Range: 0-120 seconds; 0 seconds)
- **Priority** – The priority of this router in a VRRP group. (Range: 1-254; Default: 100)
  - The priority for the VRRP group address owner is automatically set to 255.
  - The priority for backup routers is used to determine which router will take over as the acting master router if the current master fails.
- **Authentication Type** – Authentication mode used to verify VRRP packets received from other routers. (Options: None, Simple Text)
  - If simple text authentication is selected, then you must also enter an authentication string.
  - All routers in the same VRRP group must be set to the same authentication mode, and be configured with the same authentication string.
  - Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.
- **Authentication String** – Key used to authenticate VRRP packets received from other routers. (Range: 1-8 alphanumeric characters)
  - When a VRRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.

Web – Click IP, VRRP, Group Configuration. Select the VLAN ID, enter the VRID group number, and click Add.



VRRP Group Configuration

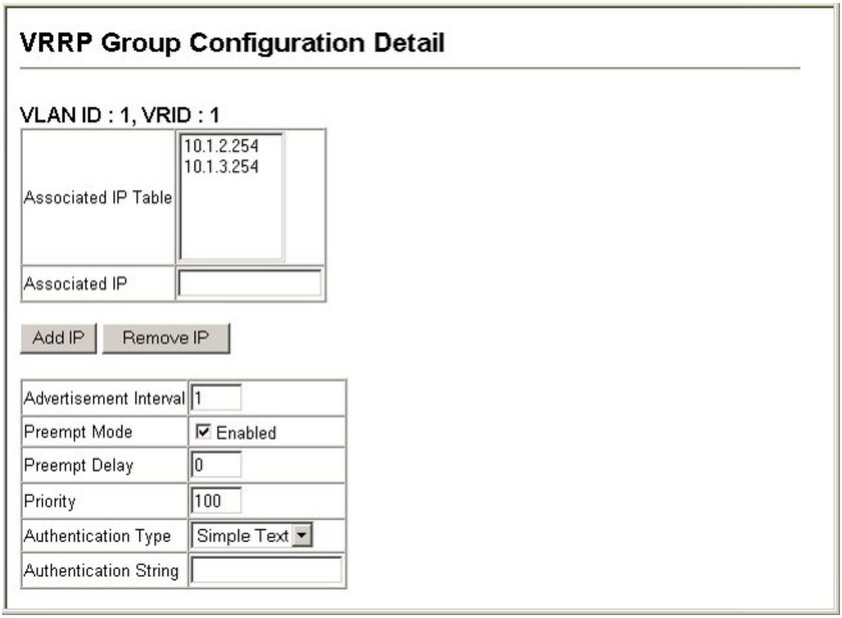
VLAN ID	VRID	State	Virtual address	Interval	Preemption	Priority	AuthType	Edit	Delete
1	1	Master	10.1.2.254	1	Enabled	100	Simple Text	Edit	Delete
1	1	Master	10.1.3.254	1	Enabled	100	Simple Text	Edit	Delete
1	5	Master	10.1.1.254	1	Enabled	100	Simple Text	Edit	Delete

Total VRRP group: 1

VLAN ID	1
VRID	

Figure 18-1 VRRP Group Configuration

Click the Edit button for a group entry to open the detailed configuration window. Enter the IP address of a real interface on this router to make it the master virtual router for the group. Otherwise, enter the virtual address for an existing group to make it a backup router, or to compete as the master based on configured priority if no other members are set as the owner of the group address. Click Add IP to enter an IP address into the Associated IP Table. Then set any of the other parameters as required, and click Apply.



VRRP Group Configuration Detail

VLAN ID : 1, VRID : 1

Associated IP Table	10.1.2.254 10.1.3.254
Associated IP	

Advertisement Interval	1
Preempt Mode	☑ Enabled
Preempt Delay	0
Priority	100
Authentication Type	Simple Text
Authentication String	

Figure 18-2 VRRP Group Configuration Detail

CLI – This example creates VRRP group 1, sets this switch as the master virtual router by assigning the primary interface address for the selected VLAN to the virtual IP address. It then adds a secondary IP address to the VRRP group, sets all of the other VRRP parameters, and then displays the configured settings.

```
Console(config)#interface vlan 1                                        27-1
Console(config-if)#vrrp 1 ip 192.168.1.6                                40-2
Console(config-if)#vrrp 1 ip 192.168.2.6 secondary
Console(config-if)#vrrp 1 timers advertise 5                            40-4
Console(config-if)#vrrp 1 preempt delay 10                              40-5
Console(config-if)#vrrp 1 priority 1                                    40-3
Console(config-if)#vrrp 1 authentication bluebird                       40-3
Console(config-if)#end
Console#show vrrp                                                       40-6
 Vlan 1 - Group 1,
 State                            Master
 Virtual IP Address              192.168.1.6
 Virtual MAC Address             00-00-5E-00-01-01
 Advertisement Interval          5 sec
 Preemption                      enabled
 Min Delay                       10 sec
 Priority                        1
 Authentication                  SimpleText
 Authentication Key              bluebird
 Master Router                   192.168.1.6
 Master Priority                 255
 Master Advertisement Interval   5 sec
 Master Down Interval            15
Console#
```

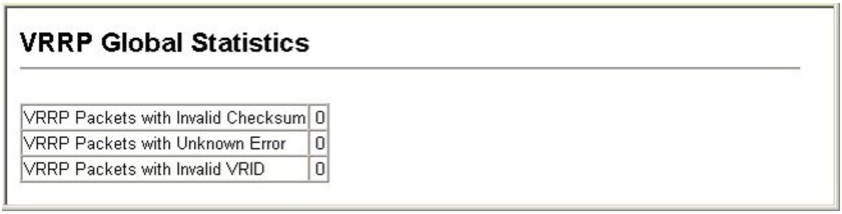
Displaying VRRP Global Statistics

The VRRP Global Statistics page displays counters for errors found in VRRP protocol packets.

Field Attributes

- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number of VRRP packets received with an invalid VRID for this virtual router.

Web – Click IP, VRRP, Global Statistics.



VRRP Global Statistics

VRRP Packets with Invalid Checksum	0
VRRP Packets with Unknown Error	0
VRRP Packets with Invalid VRID	0

Figure 18-3 VRRP Global Statistics

CLI – This example displays counters for protocol errors for all the VRRP groups configured on this switch.

```
Console#show vrrp router counters                                     40-9
  VRRP Packets with Invalid Checksum : 0
  VRRP Packets with Unknown Error      : 0
  VRRP Packets with Invalid VRID       : 0
Console#
```

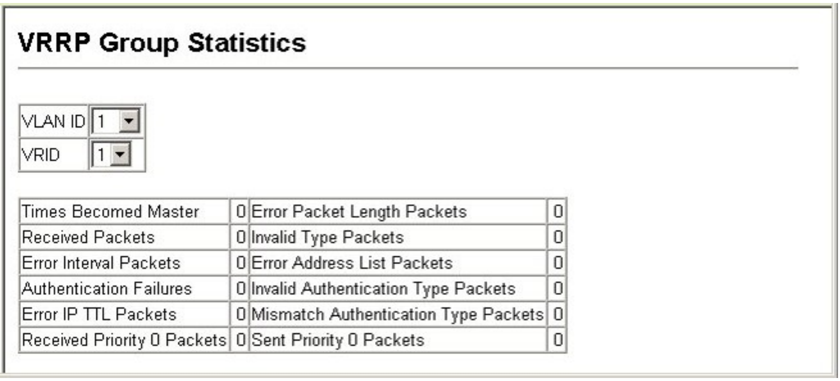
Displaying VRRP Group Statistics

The VRRP Group Statistics page displays counters for VRRP protocol events and errors that have occurred on a specific VRRP interface.

Field Attributes

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4093; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **Times Become Master** – Number of times this router has transitioned to master.
- **Received Packets** – Number of VRRP advertisements received by this router.
- **Error Interval Packets** – Number of VRRP advertisements received for which the advertisement interval is different from the one configured for the local virtual router.
- **Authentication Failures** – Number of VRRP packets received that do not pass the authentication check.
- **Error IP TTL Packets** – Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
- **Received Priority 0 Packets** – Number of VRRP packets received by the virtual router with priority set to 0.
- **Error Packet Length Packets** – Number of packets received with a packet length less than the length of the VRRP header.
- **Invalid Type Packets** – Number of VRRP packets received by the virtual router with an invalid value in the “type” field.
- **Error Address List Packets** – Number of packets received for which the address list does not match the locally configured list for the virtual router.
- **Invalid Authentication Type Packets** – Number of packets received with an unknown authentication type.
- **Mismatch Authentication Type Packets** – Number of packets received with “Auth Type” not equal to the locally configured authentication method.
- **Sent Priority 0 Packets** – Number of VRRP packets sent by the virtual router with priority set to 0. A priority value of zero indicates that the group master has stopped participating in VRRP, and is used to quickly transition a backup unit to master mode without having to wait for the master to time out.

Web – Click IP, VRRP, Group Statistics. Select the VLAN and virtual router group.



VRRP Group Statistics

VLAN ID	1
VRID	1

Times Becomed Master	0	Error Packet Length Packets	0
Received Packets	0	Invalid Type Packets	0
Error Interval Packets	0	Error Address List Packets	0
Authentication Failures	0	Invalid Authentication Type Packets	0
Error IP TTL Packets	0	Mismatch Authentication Type Packets	0
Received Priority 0 Packets	0	Sent Priority 0 Packets	0

Figure 18-4 VRRP Group Statistics

CLI – This example displays VRRP protocol statistics for group 1, VLAN 1.

```
Console#show vrrp 1 interface vlan 1 counters                         40-9
 Total Number of Times Transitioned to MASTER                        : 6
 Total Number of Received Advertisements Packets                     : 0
 Total Number of Received Error Advertisement Interval Packets       : 0
 Total Number of Received Authentication Failures Packets            : 0
 Total Number of Received Error IP TTL VRRP Packets                  : 0
 Total Number of Received Priority 0 VRRP Packets                    : 0
 Total Number of Sent Priority 0 VRRP Packets                        : 5
 Total Number of Received Invalid Type VRRP Packets                  : 0
 Total Number of Received Error Address List VRRP Packets            : 0
 Total Number of Received Invalid Authentication Type VRRP Packets  : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets : 0
 Total Number of Received Error Packet Length VRRP Packets           : 0
Console#
```

Chapter 19: IP Routing

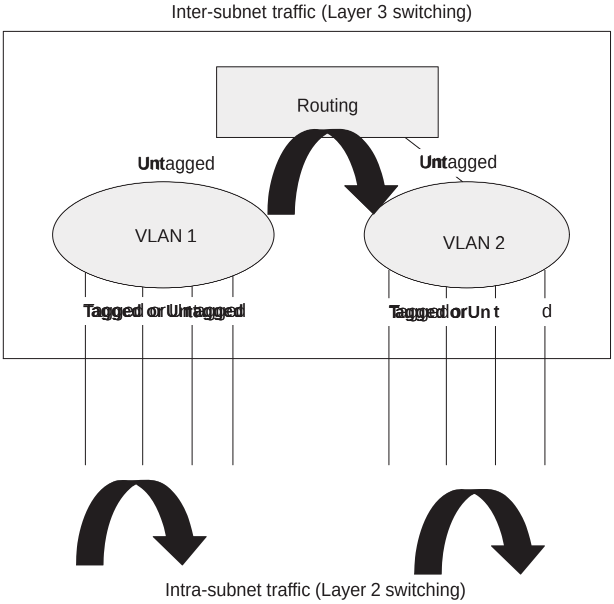
Overview

This switch supports IP routing and routing path management via static routing definitions (page 19-21) and dynamic routing protocols such as RIP or OSPF (page 20-2 or 20-14, respectively). When IP routing is enabled (page 19-4), this switch acts as a wire-speed router, passing traffic between VLANs with different IP interfaces, and routing traffic to external IP networks. However, when the switch is first booted, default routing can only forward traffic between local interfaces. As with all traditional routers, the static and dynamic routing functions must first be configured to work.

Initial Configuration

By default, all ports belong to the same VLAN and the switch provides only Layer 2 functionality. To segment the attached network, first create VLANs for each unique user group or application traffic (page 11-6), assign all ports that belong to the same group to these VLANs (page 11-7), and then assign an IP interface to each VLAN (page 19-5). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. You just need to provide the network address for each virtual interface, and the traffic between different subnetworks will be routed by Layer 3 switching.


Inter-subnet traffic (Layer 3 switching)
Routing
Untagged
Untagged
VLAN 1
VLAN 2
Tagged or Untagged
Tagged or Unt d
Intra-subnet traffic (Layer 2 switching)

IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
  - Based on the Layer 3 destination address
  - Replacing destination/source MAC addresses for each hop
  - Incrementing the hop count
  - Decrementing the time-to-live
  - Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on this switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on this switch, then the packet should be sent to the next hop router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node through the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

Note: In order to perform IP switching, the switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router via the ICMP process.

When the switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

Routing Protocols

The switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the switch either manually or when a connection is set up by an application outside the switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

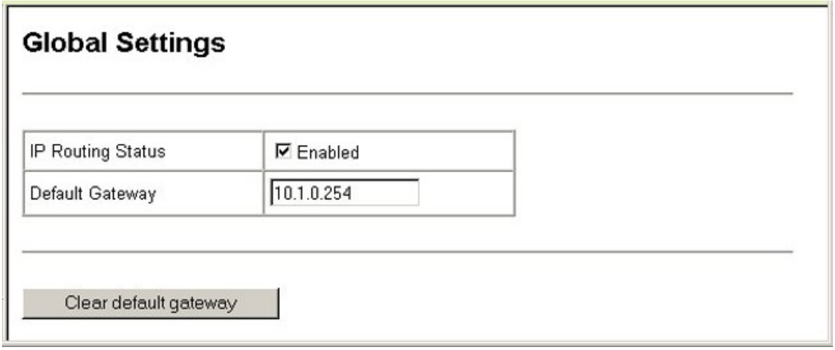
Basic IP Interface Configuration

To allow routing between different IP subnets, you must enable IP Routing as described in this section. You also need to you define a VLAN for each IP subnet that will be connected directly to this switch. Note that you must first create a VLAN as described under “Creating VLANs” on page 11-6 before configuring the corresponding subnet. Remember that if you need to manage the switch in-band then you must define the IP subnet address for at least one VLAN.

Command Attributes

- **IP Routing Status** – Configures the switch to operate as a Layer 2 switch or as a multilayer routing switch. (Options: Disable this field to restrict operation to Layer 2 switching; enable it to allow multilayer operation at either Layer 2 or 3 as required.)
  - This command affects both static and dynamic unicast routing.
  - If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.
- **Default Gateway** – The routing device to which the switch will pass packets for all unknown subnets; i.e., packets that do not match any routing table entry. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

Web - Click IP, General, Global Settings. Set IP Routing Status to Disabled to restrict operation to Layer 2, or Enabled to allow multilayer switching, specify the default gateway which will be forwarded packets for all unknown subnets, and click Apply.



Global Settings

IP Routing Status	☑ Enabled
Default Gateway	10.1.0.254

Figure 19-1 IP Global Settings

CLI - This example enables IP routing, and sets the default gateway.

```
Console(config)#ip routing                                        42-1
Console(config)#ip route default 10.1.0.254                       42-2
Console(config)#
```

Configuring IP Routing Interfaces

You can specify the IP subnets connected to this router by manually assigning an IP address to each VLAN, or by using the RIP or OSPF dynamic routing protocols to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Once IP interfaces have been configured, the switch functions as a multilayer routing switch, operating at either Layer 2 or 3 as required. All IP packets are routed directly between local interfaces, or indirectly to remote interfaces using either static routing or dynamic routing. All other packets for non-IP protocols (for example, NetBuei, NetWare or AppleTalk) are switched based on MAC addresses.

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes through shared media) that will be assigned to a specific subnet, then you must create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network prefix number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network segment that is connected to that interface, and allows you to send IP packets to or from the router.

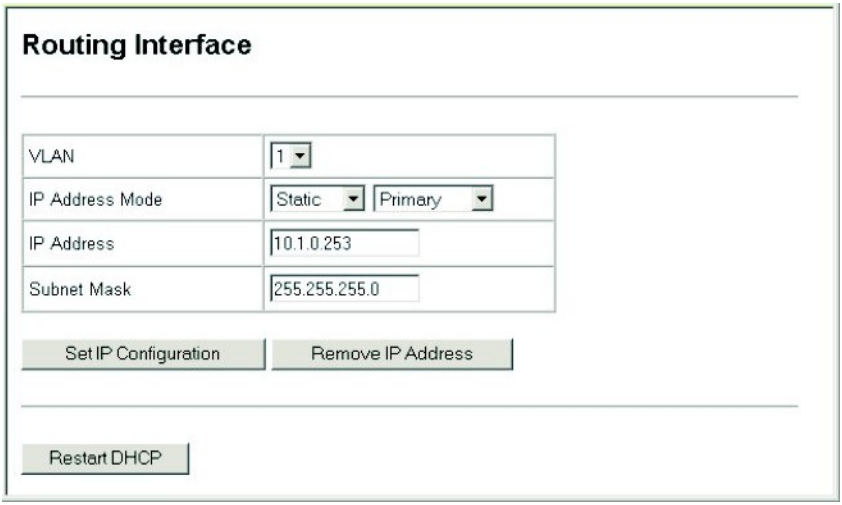
- Before you configure any network interfaces on this router, you should first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- An IP address must be assigned to gain management access over the network or to connect the switch to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4093).
- **IP Address Mode** – Specifies whether the IP address for this interface is statically assigned, or obtained from a network address server. (Options: Static, DHCP - Dynamic Host Configuration Protocol, BOOTP - Boot Protocol; Default: Static)
  - If Static address type is selected, then you must also specify whether the IP address is the primary IP address on the VLAN or a secondary IP address. An interface can have only one primary IP address, but can have multiple secondary IP addresses. In other words, you will need to specify secondary addresses if more than one IP subnet can accessed via this interface.
  - If DHCP/BOOTP is enabled, the system will immediately start broadcasting service requests. IP is enabled but does not function until a reply has been received from the address server. Requests will be broadcast periodically by the router for an IP address. (DHCP/BOOTP values can include the IP address, default gateway, and subnet mask.)
- **IP Address** – Address of the VLAN interface. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the network portion of the address used for routing to specific subnets.
- **Secondary** – If Static address type is selected, the IP address can be the primary IP address on the VLAN or a secondary IP address. An interface can have only one primary IP address, but can have multiple secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface.

  Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router in a network segment uses a secondary address, all other routers in that segment must also use a secondary address from the same network or subnet address space.

Web - Click IP, General, Routing Interface. Specify an IP interface for each VLAN that will support routing to other subnets. First specify a primary address, and click Set IP Configuration. If you need to assign secondary addresses, enter these addresses one at a time, and click Set IP Configuration after entering each address.


Routing Interface

VLAN	1
IP Address Mode	Static Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0

Figure 19-2 IP Routing Interface

CLI - This example sets a primary IP address for VLAN 1, and then adds a secondary IP address for a different subnet also attached to this router interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.253 255.255.255.0          41-3
Console(config-if)#ip address 10.1.9.253 255.255.255.0 secondary
Console(config-if)#
```

Address Resolution Protocol

If IP routing is enabled (page 19-4), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (i.e., MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

Table 19-1 Address Resolution Protocol

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

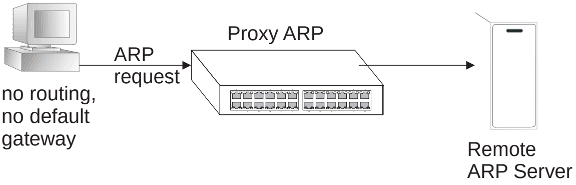
Basic ARP Configuration

You can use the ARP General configuration menu to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

Command Usage

Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.



Command Attributes

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)

  The ARP aging timeout can be set for any currently configured VLAN.

  The aging time determines how long dynamic entries remain the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.

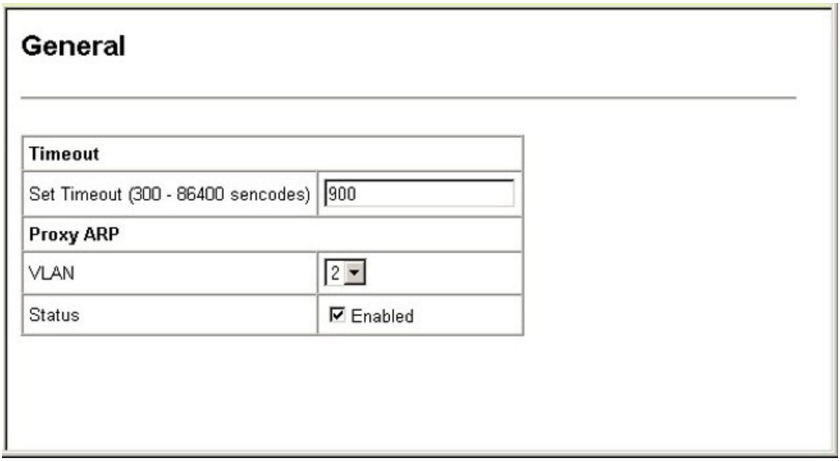
  When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.

- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces, allowing a non-routing device to determine the MAC address of a host on another subnet or network. (Default: Disabled)

  End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.

  Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Web - Click IP, ARP, General. Set the timeout to a suitable value for the ARP cache, enable Proxy ARP for subnetworks that do not have routing or a default gateway, and click Apply.



General

Timeout	
Set Timeout (300 - 86400 sencodes)	900
Proxy ARP	
VLAN	2
Status	☑ Enabled

Figure 19-3 ARP General

CLI - This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds), and enables Proxy ARP for VLAN 3.

```
Console(config)#arp-timeout 900                                        41-33
Console(config)#interface vlan 3                                        27-1
Console(config-if)#ip proxy-arp                                        41-35
Console(config-if)#
```

Configuring Static ARP Addresses

For devices that do not respond to ARP requests or do not respond in a timely manner, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, you can manually map an IP address to the corresponding physical address in the ARP cache.

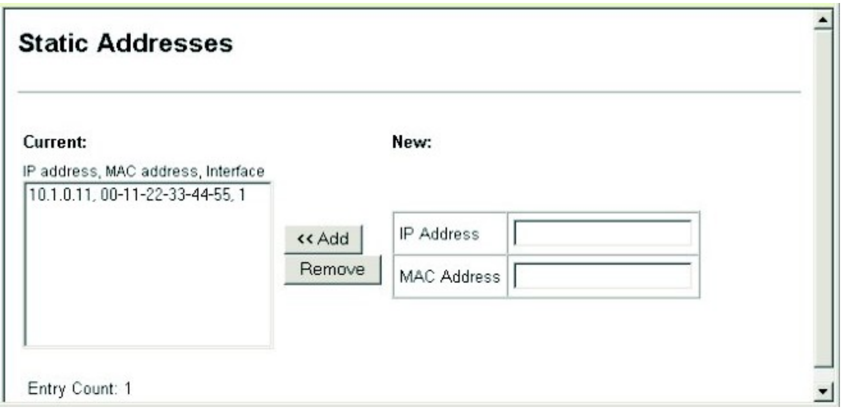
Command Usage

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (that is, Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- You can define up to 128 static entries in the ARP cache.
- A static entry may need to be used if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.
- Static entries will not be aged out or deleted when power is reset. You can only remove a static entry via the configuration interface.

Command Attributes

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx.)
- **Entry Count** – The number of static entries in the ARP cache.

Web - Click IP, ARP, Static Addresses. Enter the IP address, the corresponding MAC address, and click Apply.



Static Addresses

Current:

IP address, MAC address, Interface

10.1.0.11, 00-11-22-33-44-55, 1

New:

IP Address	
MAC Address	

Entry Count: 1

Figure 19-4 ARP Static Addresses

CLI - This example sets a static entry for the ARP cache.

```
Console(config)#arp 10.1.0.11 00-11-22-33-44-55                          41-32
Console(config)#exit
Console#show arp
Arp cache timeout: 1200 (seconds)

    IP Address         MAC Address       Type    Interface
--------------- ---------------- --------- -----------
192.168.0.4      00-E0-29-94-34-1C dynamic               1
10.1.0.11        00-11-22-33-44-55 static                2

Total entry : 2
Console(config)#
```

Displaying Dynamically Learned ARP Entries

The ARP cache contains entries that map IP addresses to the corresponding physical address. The ARP cache contains static entries, and entries for local interfaces, including subnet, host, and broadcast addresses. Most of these entries will be dynamically learned through replies to broadcast messages. You can display all of the dynamic entries in the ARP cache, change specific dynamic entries into static entries, or clear all dynamic entries from the cache.

Command Attributes

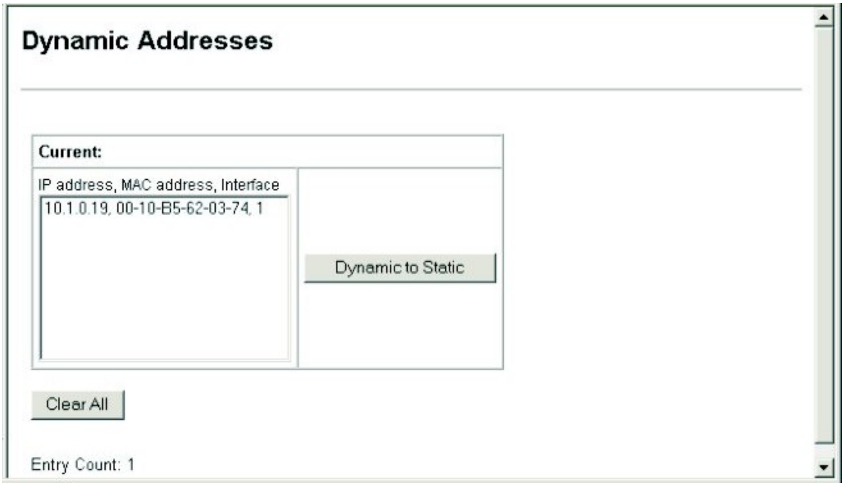
- **IP Address** – IP address of a dynamic entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Dynamic to Static**[19] – Changes a selected dynamic entry to a static entry.
- **Clear All**[19] – Deletes all dynamic entries from the ARP cache.
- **Entry Count** – The number of dynamic entries in the ARP cache.

The following field is also displayed in the CLI.

- **Type** – Indicates if entries were learned through replies to broadcast messages, are statically configured entries, or are other entries for local interfaces (including subnet and broadcast addresses).

[19] These buttons take effect immediately. You are not prompted to confirm the action.

Web - Click IP, ARP, Dynamic Addresses. You can use the buttons provided to change a dynamic entry to a static entry, or to clear all dynamic entries in the cache.



10.1.0.19, 00-10-B5-62-03-74, 1

Entry Count: 1

Figure 19-5 ARP Dynamic Addresses

CLI - This example shows all entries in the ARP cache.

```
Console#show arp                                                    41-34
Arp cache timeout: 1200 (seconds)

    IP Address        MAC Address       Type    Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff      other           1
      10.1.0.11 00-11-22-33-44-55     static           1
      10.1.0.12 01-02-03-04-05-06     static           1
      10.1.0.19 00-10-b5-62-03-74    dynamic           1
     10.1.0.253 00-00-ab-cd-00-00      other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff      other           1

Total entry : 6
Console#clear arp-cache                                             41-34
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

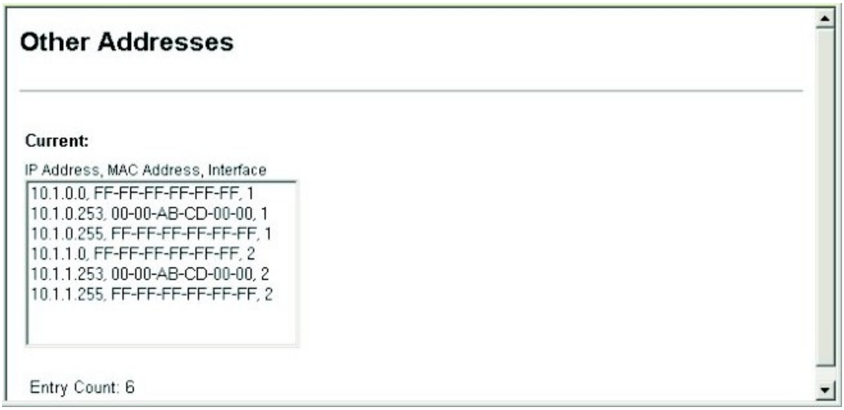
Displaying Local ARP Entries

The ARP cache also contains entries for local interfaces, including subnet, host, and broadcast addresses.

Command Attributes

- **IP Address** – IP address of a local entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Entry Count** – The number of local entries in the ARP cache.

Web - Click IP, ARP, Other Addresses.



Other Addresses

Current:

IP Address, MAC Address, Interface

10.1.0.0, FF-FF-FF-FF-FF-FF, 1
10.1.0.253, 00-00-AB-CD-00-00, 1
10.1.0.255, FF-FF-FF-FF-FF-FF, 1
10.1.1.0, FF-FF-FF-FF-FF-FF, 2
10.1.1.253, 00-00-AB-CD-00-00, 2
10.1.1.255, FF-FF-FF-FF-FF-FF, 2

Entry Count: 6

Figure 19-6 ARP Other Addresses

CLI - This router uses the Type specification “other” to indicate local cache entries in the ARP cache.

```
Console#show arp                                                             41-34
Arp cache timeout: 1200 (seconds)

    IP Address        MAC Address       Type    Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff       other           1
      10.1.0.11 00-11-22-33-44-55    static           1
      10.1.0.12 01-02-03-04-05-06    static           1
      10.1.0.19 00-10-b5-62-03-74   dynamic           1
     10.1.0.253 00-00-ab-cd-00-00     other           1
     10.1.0.255 ff-ff-ff-ff-ff-ff     other           1

Total entry : 6
Console#
```

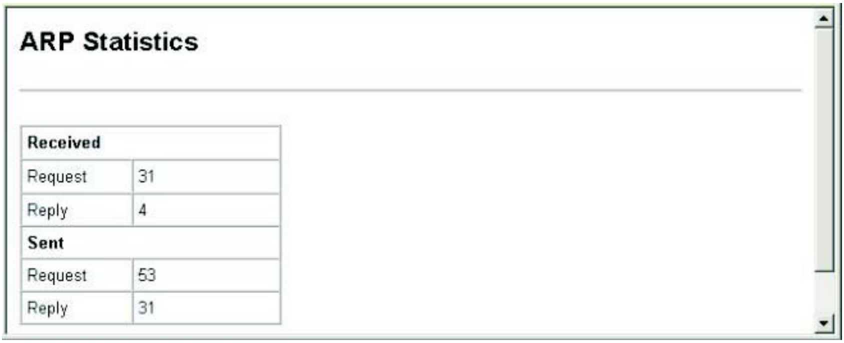
Displaying ARP Statistics

You can display statistics for ARP messages crossing all interfaces on this router.

Table 19-2 ARP Statistics

Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

Web - Click IP, ARP, Statistics.



ARP Statistics

Received	
Request	31
Reply	4
Sent	
Request	53
Reply	31

Figure 19-7 ARP Statistics

CLI - This example provides detailed statistics on common IP-related protocols.

```
Console#show ip traffic                                                     42-5
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:   9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#
```

Displaying Statistics for IP Protocols

IP Statistics

The Internet Protocol (IP) provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (i.e., hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through "small packet" networks.

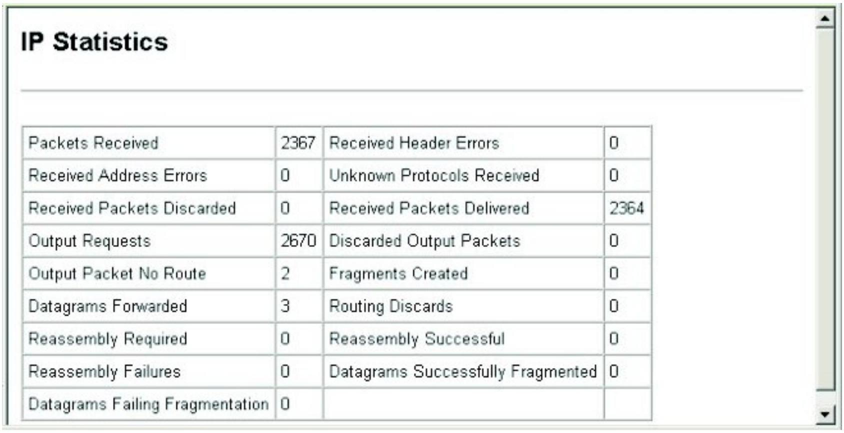
Table 19-3 IP Statistics

Parameter	Description
Packets Received	The total number of input datagrams received from interfaces, including those received in error.
Received Address Errors	The number of input datagrams discarded because the IP address in the header's destination field was not a valid address for this entity.
Received Packets Discarded	The number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).
Output Requests	The total number of datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
Output Packet No Route	The number of datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
Datagrams Forwarded	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
Reassembly Required	The number of IP fragments received which needed to be reassembled at this entity.
Reassembly Failures	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc.).
Datagrams Failing Fragmentation	The number of datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their "Don't Fragment" flag was set.
Received Header Errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.
Unknown Protocols Received	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Received Packets Delivered	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Discarded Output Packets	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).
Fragments Created	The number of datagram fragments that have been generated as a result of fragmentation at this entity.

Table 19-3 IP Statistics (Continued)

Parameter	Description
Routing Discards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
Reassembly Successful	The number of datagrams successfully re-assembled.
Datagrams Successfully Fragmented	The number of IP datagrams that have been successfully fragmented at this entity.

Web - Click IP, Statistics, IP.



IP Statistics

Packets Received	2367	Received Header Errors	0
Received Address Errors	0	Unknown Protocols Received	0
Received Packets Discarded	0	Received Packets Delivered	2364
Output Requests	2670	Discarded Output Packets	0
Output Packet No Route	2	Fragments Created	0
Datagrams Forwarded	3	Routing Discards	0
Reassembly Required	0	Reassembly Successful	0
Reassembly Failures	0	Datagrams Successfully Fragmented	0
Datagrams Failing Fragmentation	0		

Figure 19-8 IP Statistics

CLI - See the example on page 19-14.

ICMP Statistics

Internet Control Message Protocol (ICMP) is a network layer protocol that transmits message packets to report errors in processing IP packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (i.e., the next hop router) to use for a specific destination.

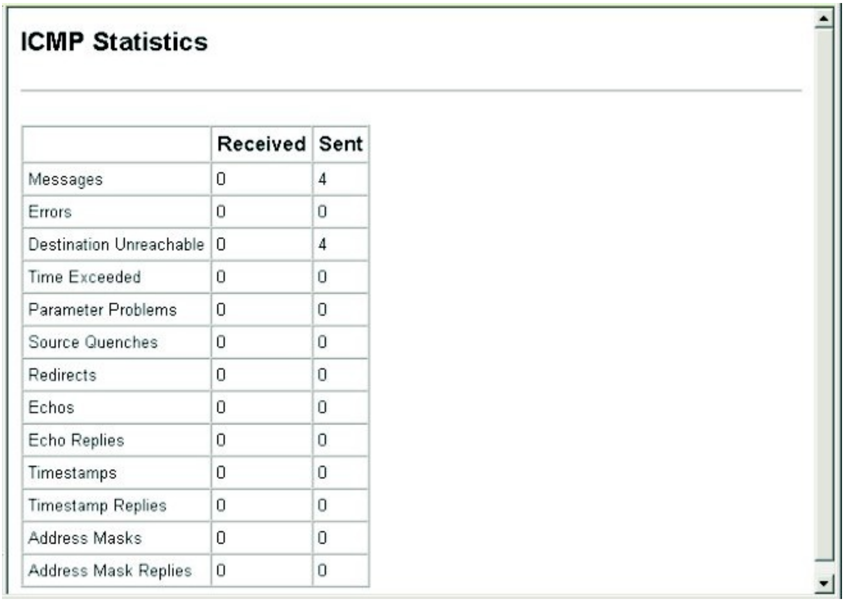
Table 19-4 ICMP Statistics

Parameter	Description
Messages	The total number of ICMP messages which the entity received/sent.
Errors	The number of ICMP messages which the entity received/sent but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

Table 19-4 ICMP Statistics (Continued)

Parameter	Description
Destination Unreachable	The number of ICMP Destination Unreachable messages received/sent.
Time Exceeded	The number of ICMP Time Exceeded messages received/sent.
Parameter Problems	The number of ICMP Parameter Problem messages received/sent.
Source Quenches	The number of ICMP Source Quench messages received/sent.
Redirects	The number of ICMP Redirect messages received/sent.
Echos	The number of ICMP Echo (request) messages received/sent.
Echo Replies	The number of ICMP Echo Reply messages received/sent.
Timestamps	The number of ICMP Timestamp (request) messages received/sent.
Timestamp Replies	The number of ICMP Timestamp Reply messages received/sent.
Address Masks	The number of ICMP Address Mask Request messages received/sent.
Address Mask Replies	The number of ICMP Address Mask Reply messages received/sent.

Web - Click IP, Statistics, ICMP.



ICMP Statistics

	Received	Sent
Messages	0	4
Errors	0	0
Destination Unreachable	0	4
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echos	0	0
Echo Replies	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

Figure 19-9 ICMP Statistics

CLI - See the example on page 19-14.

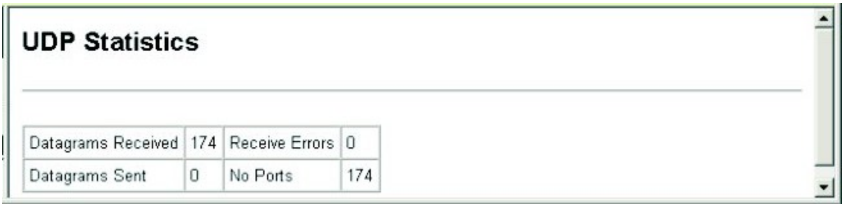
UDP Statistics

User Datagram Protocol (UDP) provides a datagram mode of packet-switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Table 19-5 USP Statistics

Parameter	Description
Datagrams Received	The total number of UDP datagrams delivered to UDP users.
Datagrams Sent	The total number of UDP datagrams sent from this entity.
Receive Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Web - Click IP, Statistics, UDP.



UDP Statistics

Datagrams Received	174	Receive Errors	0
Datagrams Sent	0	No Ports	174

Figure 19-10 UDP Statistics

CLI - See the example on page 19-14.

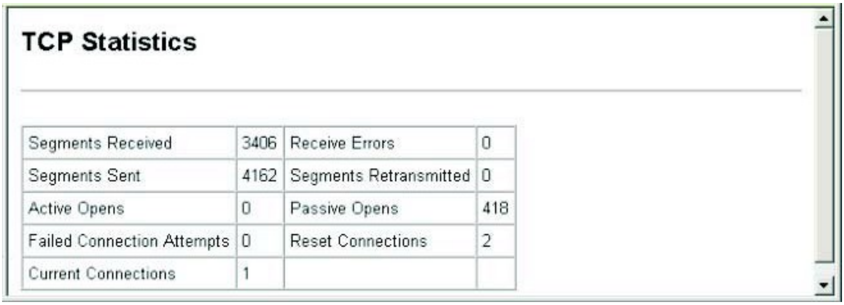
TCP Statistics

The Transmission Control Protocol (TCP) provides highly reliable host-to-host connections in packet-switched networks, and is used in conjunction with IP to support a wide variety of Internet protocols.

Table 19-6 TCP Statistics

Parameter	Description
Segments Received	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Segments Sent	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Failed Connection Attempts	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Current Connections	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE- WAIT.
Receive Errors	The total number of segments received in error (e.g., bad TCP checksums).
Segments Retransmitted	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Reset Connections	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Web - Click IP, Statistics, TCP.



TCP Statistics

Segments Received	3406	Receive Errors	0
Segments Sent	4162	Segments Retransmitted	0
Active Opens	0	Passive Opens	418
Failed Connection Attempts	0	Reset Connections	2
Current Connections	1		

Figure 19-11 TCP Statistics

CLI - See the example on page 19-14.

Configuring Static Routes

This router can dynamically configure routes to other network segments using dynamic routing protocols (i.e., RIP or OSPF). However, you can also manually enter static routes in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so you should only configure a small number of stable routes to ensure network accessibility.

Command Usage

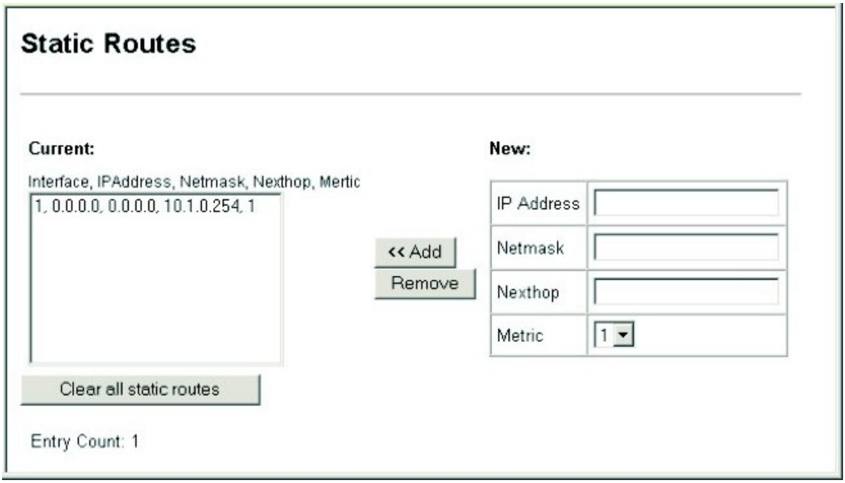
- Up to 64 static routes can be configured.
- If a static route is defined, it will always take preference over a dynamic route.
- Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by the RIP or OSPF (see page 20-9 or 20-35, respectively).

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Gateway** – IP address of the next router hop used for this route.
- **Metric** – Cost for this interface. (Range: 1-5, Default: 1)

  The metric is an administrative distance, and indicates that this route can be overridden by dynamic routing information if the distance of the dynamic route is less than that configured for the static route. Note that the default administrative distances used by the dynamic unicast routing protocols is 110 for OSPF and 120 for RIP.
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Static Routes.



Static Routes

Current:

Interface, IPAddress, Netmask, Nexthop, Mertic

1, 0.0.0.0, 0.0.0.0, 10.1.0.254, 1

New:

IP Address	
Netmask	
Nexthop	
Metric	1

Entry Count: 1

Figure 19-12 IP Static Routes

CLI - This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254     42-2
Console(config)#
```

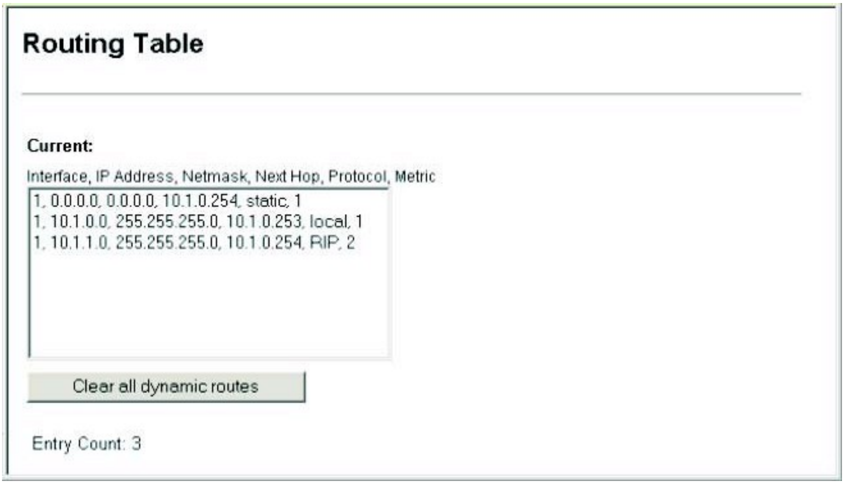
Displaying the Routing Table

You can display all the routes that can be accessed via the local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic. Also note that the route for a local interface is not enabled (i.e., listed in the routing table) unless there is at least one active link connected to that interface.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – The IP address of the next hop (or gateway) in this route.
- **Protocol** – The protocol which generated this route information. (Options: Local, Static, RIP, OSPF)
- **Metric** – Cost for this interface.
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Routing Table.



Routing Table

Current:

Interface, IP Address, Netmask, Next Hop, Protocol, Metric

```
1, 0.0.0.0, 0.0.0.0, 10.1.0.254, static, 1
1, 10.1.0.0, 255.255.255.0, 10.1.0.253, local, 1
1, 10.1.1.0, 255.255.255.0, 10.1.0.254, RIP, 2
```

Entry Count: 3

Figure 19-13 IP Routing Table

CLI - This example shows routes obtained from various methods.

```
Console#show  ip  route                                                      42-3

  Ip Address         Netmask           Next Hop       Protocol Metric Interface
--------------- --------------- --------------- -------- ------ ---------
        0.0.0.0         0.0.0.0      10.1.0.254    static       1         1
       10.1.0.0   255.255.255.0      10.1.0.253     local       1         1
       10.1.1.0   255.255.255.0      10.1.0.254       RIP       2         1

Total entries: 3
Console#
```

Chapter 20: Unicast Routing

This switch can route unicast traffic to different subnetworks using the Routing Information Protocol (RIP) or Open Shortest Path First (OSPF) protocol. It supports RIP, RIP-2 or OSPFv2 dynamic routing. These protocols exchange routing information, calculate routing tables, and can respond to changes in the status or loading of the network.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

OSPFv2 Dynamic Routing Protocol

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

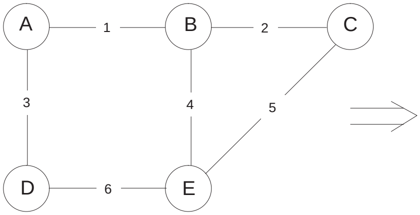
Non-IP Protocol Routing

The switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by this switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

Configuring the Routing Information Protocol

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.



Cost = 1 for all links

A	Link	Cost
A	0	0
B	1	1
C	1	2
D	3	1
E	1	2

Routing table for node A

Command Usage

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:
  - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
  - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
  - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.
- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).
- There are several serious problems with RIP that you should consider. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information via broadcasts; it also considers too few network variables to make the best routing decision.

Configuring General Protocol Settings

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, you need to specify the RIP version used globally by the router, as well as the RIP send and receive versions used on specific interfaces (page 20-6).

Command Attributes

Global Settings

- **RIP Routing Process** – Enables RIP routing for all IP interfaces on the router. (Default: Disabled)
- **Global RIP Version** – Specifies a RIP version used globally by the router. (Default: RIP Version 1)

  When you specify a Global RIP Version, any VLAN interface not previously set to a specific Receive or Send Version (page 20-6) is set to the following values:

  - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.

  RIP send/receive versions set on the RIP Interface Settings screen (page 20-6) always take precedence over the settings for the Global RIP Version.

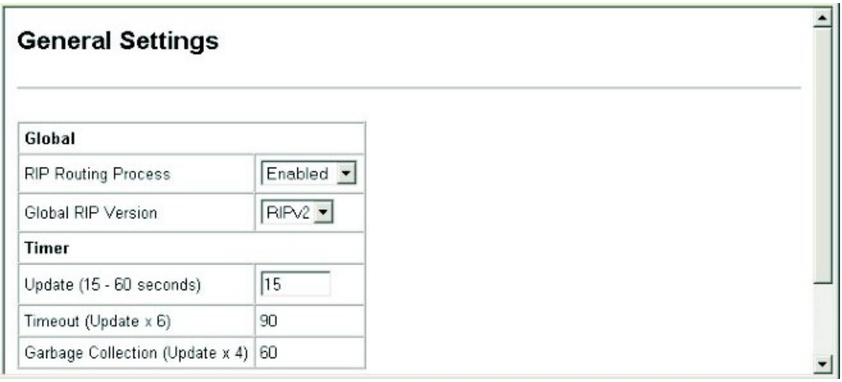
Timer Settings

The timers must be set to the same values for all routers in the network.

- **Update** – Sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes. This value will also set the timeout timer to 6 times the update time, and the garbage-collection timer to 4 times the update time. (Range: 15-60 seconds; Default: 30 seconds)

  Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.
- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. (Default: 180 seconds)
- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. (Default: 120 seconds)

Web - Click Routing Protocol, RIP, General Settings. Enable or disable RIP, set the RIP version used on previously unset interfaces to RIPv1 or RIPv2, set the basic update timer, and then click Apply.



General Settings

Global	
RIP Routing Process	Enabled
Global RIP Version	RIPv2
Timer	
Update (15 - 60 seconds)	15
Timeout (Update x 6)	90
Garbage Collection (Update x 4)	60

Figure 20-1 RIP General Settings

CLI - This example sets the router to use RIP Version 2, and sets the basic timer to 15 seconds.

```
Console(config)#router rip                                          42-6
Console(config-router)#version 2                                   42-11
Console(config-router)#timers basic 15                              42-8
Console(config-router)#end
Console#show rip globals                                           42-16

RIP Process: Enabled
Update Time in Seconds: 15
Number of Route Change: 0
Number of Queries: 1
Console#
```

Specifying Network Interfaces for RIP

You must specify network interfaces that will be included in the RIP routing process.

Command Usage

- RIP only sends updates to interfaces specified by this command.

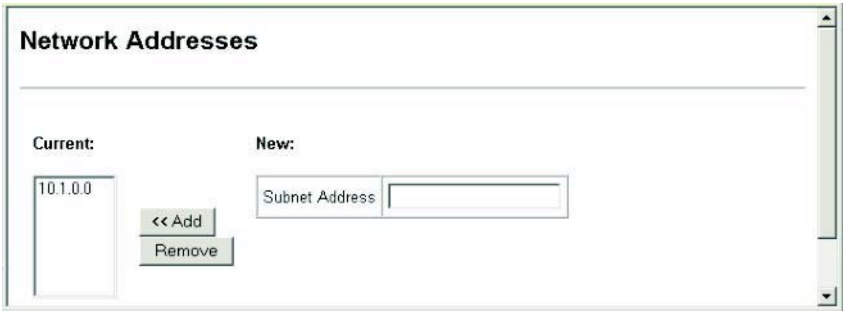
Command Attributes

- **Subnet Address** – IP address of a network directly connected to this router.

  Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:

  0 - 127 is class A, and only the first field in the network address is used.
  128 - 191 is class B, and the first two fields in the network address are used.
  192 - 223 is class C, and the first three fields in the network address are used.

Web - Click Routing Protocol, RIP, Network Addresses. Add all interfaces that will participate in RIP, and click Apply.


Network Addresses

Current:

10.1.0.0

New:

Subnet Address

Figure 20-2 RIP Network Addresses

CLI - This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config)#router-rip                                                    42-6
Console(config-router)#network 10.1.0.0                                       42-9
Console(config-router)#end
Console#show ip rip status                                                   42-16

          Peer    UpdateTime    Version    RcvBadPackets    RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.253               0              0               73
     10.1.1.253               0              0               66

Console#
```

Configuring Network Interfaces for RIP

For each interface that participates in the RIP routing process, you must specify the protocol message type accepted (i.e., RIP version) and the message type sent (i.e., RIP version or compatibility mode), the method for preventing loopback of protocol messages, and whether or not authentication is used (i.e., authentication only applies if RIPv2 messages are being sent or received).

Command Usage

Specifying Receive and Send Protocol Types

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified by the RIP / General Settings, Global RIP Version field.
- You can specify the Receive Version based on these options:
  - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “RIPv1 or RIPv2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.
  - Use “Do Not Receive” if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
- You can specify the Send Version based on these options:
  - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “RIPv1 Compatible” to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)
  - Use “Do Not Send” to passively monitor route information advertised by other routers attached to the network.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP utilizes the following three methods that can provide faster convergence when the network topology changes and prevent most loops from occurring:

- Split Horizon – Never propagate routes back to an interface port from which they have been acquired.
- Poison Reverse – Propagate routes back to an interface from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- Triggered Updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required.

RIPv2 supports authentication via a simple password or MD5 key encryption. When a router is configured to exchange authentication messages, it will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

Command Attributes

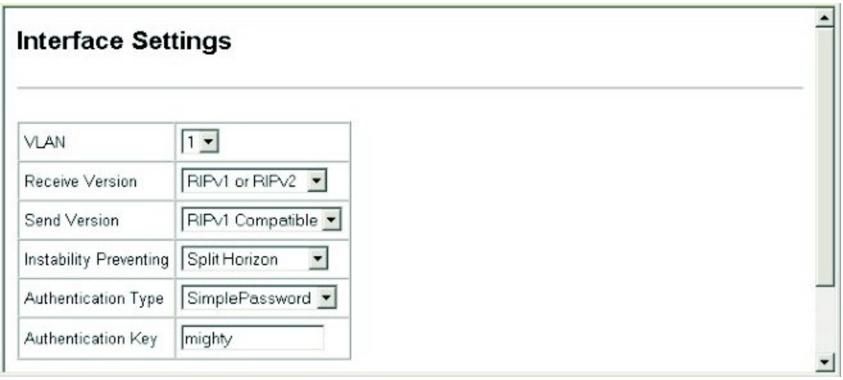
- **VLAN** – ID of configured VLAN (1-4093).
- **Receive Version** – The RIP version to receive on an interface.
  - **RIPv1**: Accepts only RIPv1 packets.
  - **RIPv2**: Accepts only RIPv2 packets.
  - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets. (Default[20])
  - **Do Not Receive**: Does not accept incoming RIP packets. This option does not add any dynamic entries to the routing table for an interface.
- **Send Version** – The RIP version to send on an interface.
  - **RIPv1**: Sends only RIPv1 packets.
  - **RIPv2**: Sends only RIPv2 packets.
  - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2. (Default[20])
  - **Do Not Send**: Does not transmit RIP updates.
- **Instability Preventing** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router. (Default: None)
  - **None**: No loopback prevention method is employed. If a loop occurs, the hop count for a route may be gradually incremented to infinity (i.e., 16) before the route is deemed unreachable.
  - **Split Horizon**: This method never propagates routes back to an interface from which they have been acquired.
  - **Poison Reverse**: This method propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. This provides faster convergence.

[20] These defaults are displayed on the RIP / Interface Settings page once RIP has been enabled globally (RIP / General Settings) and an interface added to the RIP process (RIP / Network Addresses). Note that any configured interface settings take precedence over the global settings.

- **Authentication Type** – Specifies whether or not authentication is required for exchanging protocol messages. (Default: No Authentication)
  - **No Authentication**: No authentication is required.
  - **Simple Password**: Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
  - **MD5**: Message Digest 5 (MD5) authentication.

    MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given pre-specified target message digest.
- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

Web - Click Routing Protocol, RIP, Interface Settings. Select the RIP protocol message types that will be received and sent, the method used to provide faster convergence and prevent loopback (i.e., prevent instability in the network topology), and the authentication option and corresponding password. Then click Apply.



Interface Settings

VLAN	1
Receive Version	RIPv1 or RIPv2
Send Version	RIPv1 Compatible
Instability Preventing	Split Horizon
Authentication Type	SimplePassword
Authentication Key	mighty

Figure 20-3 RIP Interface Settings

CLI - This example sets the receive version to accept both RIPv1 or RIPv2 messages, the send mode to RIPv1 compatible (i.e., called v2-broadcast in the CLI), sets the method of preventing instability in the network topology to Split Horizon, enables authentication via a simple password (i.e., called text mode in the CLI).

```
Console(config)#interface vlan 1                             27-1
Console(config-if)#ip rip receive version 1 2               42-12
Console(config-if)#ip rip send version v2-broadcast         42-13
Console(config-if)#ip split-horizon                         42-14
Console(config-if)#ip rip authentication mode text          42-15
Console(config-if)#ip rip authentication key mighty         42-14
Console#
```

Redistributing Routing Information from Other Domains

RIP can be configured to import external routing information from other routing domains (that is, protocols or static routes) into the autonomous system.

Command Attributes

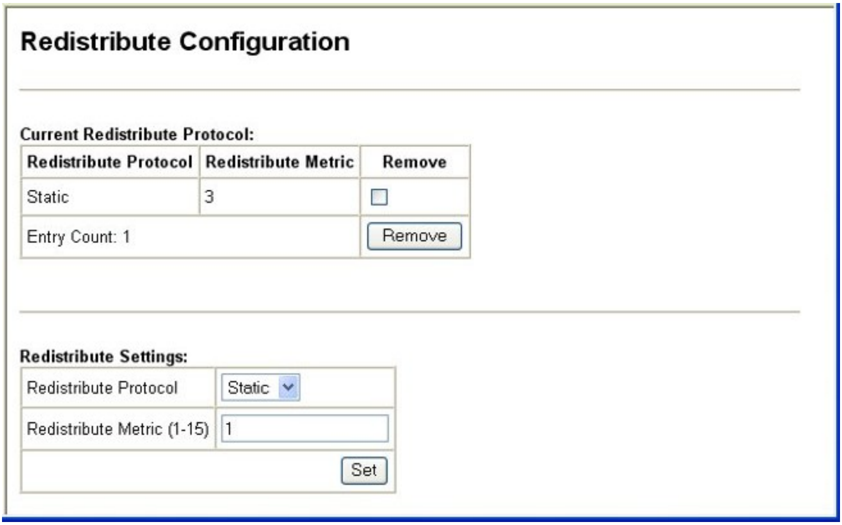
- **Redistribute Protocol** – Only static routes can be imported into this routing domain.
- **Redistribute Metric** – Metric value assigned to all external routes for the specified protocol. (Range: 1-15; Default: The default metric value is set by the **default-metric** command described on page 42-7).

  If a redistribution metric has not been configured for static routes, the **default-metric** command (page 42-7) sets the metric value to be used for all imported external routes.

  A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.

  It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

Web - Click Routing Protocol, RIP, Redistribute Configuration. Enter the redistribution metric for static routes, and click Set.



Redistribute Configuration

Current Redistribute Protocol:

Redistribute Protocol	Redistribute Metric	Remove
Static	3	□
Entry Count: 1		Remove

Redistribute Settings:

Redistribute Protocol	Static
Redistribute Metric (1-15)	1
	Set

Figure 20-4 RIP Redistribution Configuration

CLI - This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config)#router rip                                           42-6
Console(config-router)#redistribute static metric 3                  42-11
Console(config-router)#
```

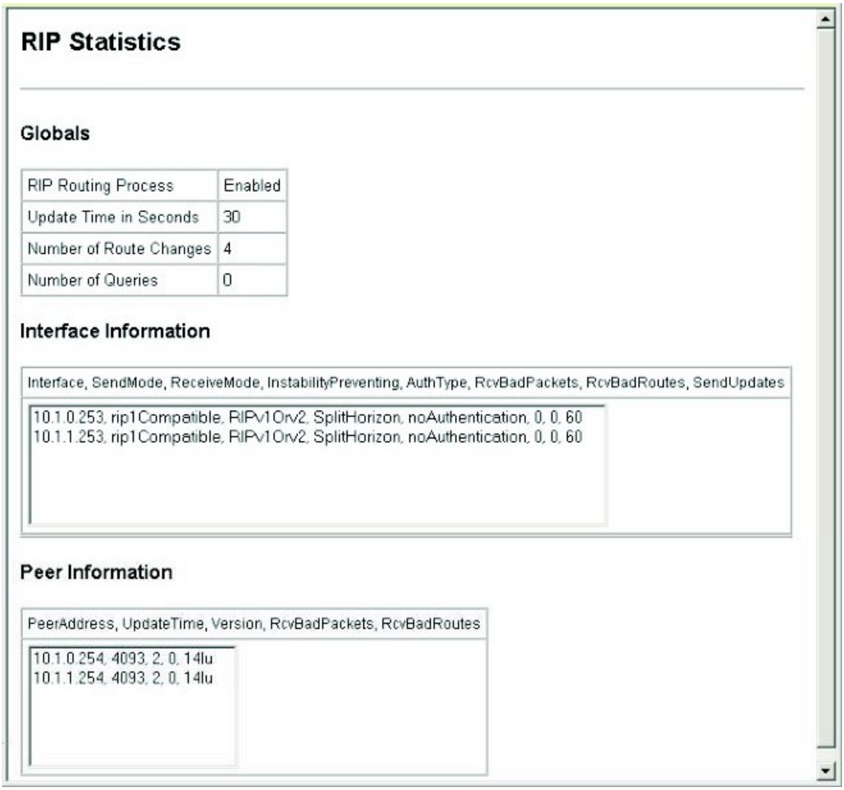
Displaying RIP Information and Statistics

You can display basic information about the current global configuration settings for RIP, statistics about route changes and queries, information about the interfaces on this router that are using RIP, and information about known RIP peer devices.

Table 20-1 RIP Information and Statistics

Parameter	Description
Globals	
RIP Routing Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.
Interface Information	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, rip1Compatible).
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1Orv2).
InstabilityPreventing	Shows if split-horizon, poison-reverse, or no instability prevention method is in use.
AuthType	Shows if authentication is set to simple password or none.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
Peer Information	
PeerAddress	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Web - Click Routing Protocol, RIP, Statistics.



RIP Statistics

Globals

RIP Routing Process	Enabled
Update Time in Seconds	30
Number of Route Changes	4
Number of Queries	0

Interface Information

Interface, SendMode, ReceiveMode, InstabilityPreventing, AuthType, RcvBadPackets, RcvBadRoutes, SendUpdates

```
10.1.0.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60
10.1.1.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60
```

Peer Information

PeerAddress, UpdateTime, Version, RcvBadPackets, RcvBadRoutes

```
10.1.0.254, 4093, 2, 0, 14lu
10.1.1.254, 4093, 2, 0, 14lu
```

Figure 20-5 RIP Statistics

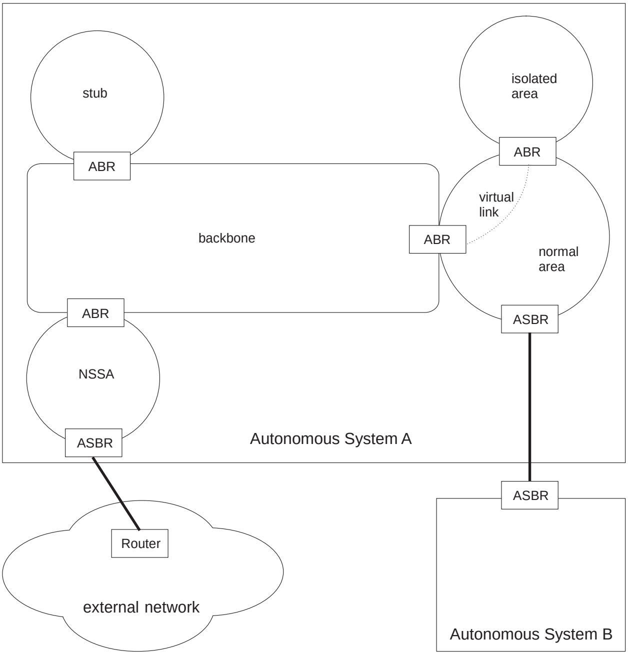
CLI - The information displayed by the RIP Statistics screen via the web interface can be accessed from the CLI using the following commands.

```
Console#show rip globals                                                  42-16

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 4
Number of Queries: 0
Console#show ip rip configuration                                         42-16

     Interface      SendMode       ReceiveMode     Poison      Authentication
--------------- --------------- ------------- -------------- ------------------
     10.1.0.253   rip1Compatible     RIPv1Orv2    SplitHorizon    noAuthentication
     10.1.1.253   rip1Compatible     RIPv1Orv2    SplitHorizon    noAuthentication
Console#show ip rip status                                                42-16

     Interface    RcvBadPackets    RcvBadRoutes      SendUpdates
--------------- --------------- -------------- ---------------
     10.1.0.253               0              0              60
     10.1.1.253               0              0              63
Console#show ip rip peer                                                  42-16

          Peer    UpdateTime    Version    RcvBadPackets    RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.254         4610         2               0              0
     10.1.1.254         4610         2               0              0
Console#
```

Configuring the Open Shortest Path First Protocol

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

Note: The OSPF protocol implemented in this device is based on RFC 2328 (Version 2). It also supports RFC 1583 (early Version 2) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older OSPF routers exist; as well as the not-so-stubby area option (RFC 3101).



Command Usage

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.

- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.
- When using OSPF, you must organize your network (i.e., autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSFP backbone.
  - To implement OSPF for a large network, you must first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). You can then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.
  - You can further optimize the exchange of OSPF traffic by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).
  - And finally, you must specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas. (Note that virtual links are not supported for stubs or NSSAs(see definition below).)

Configuring General Protocol Settings

To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached, then use the OSPF / General Configuration menu to enable OSPF, assign an Router ID to this device, and set the other basic protocol parameters.

Command Attributes

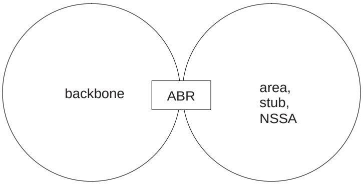
General Information –

- **OSPF Routing Process** – Enables or disables OSPF routing for all IP interfaces on the router. (Default: Disabled)
- **OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system. (Default: The lowest interface address)

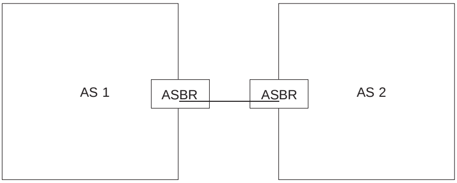
  The router ID must be unique for every router in the autonomous system. Using the default setting based on the highest interface address ensures that each router ID is unique. Also, note that the router ID cannot be set to 0.0.0.0 or 255.255.255.255.

  If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted using the **no router ospf** command followed by the **router ospf** command.
- **Version Number**[21] – The OSPF version number. The OSPF protocol implemented in this device is based on RFC 2328 (Version 2). It also supports RFC 1583 (early Version 2) compatibility mode.

[21] These items are read only.



- **Area Border Router**[21] – Indicates if this router connects directly to networks in two or more areas. An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area.



- **AS Boundary Router**[22] Autonomous System Boundary Router – Allows this router to exchange routing information with boundary routers in other autonomous systems to which it may be attached. If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device. (Default: Disabled)
- **RFC1583 Compatible** – If one or more routers in a routing domain are using early Version 2 of OSPF, this router should use RFC 1583 (early OSPFv2) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)

  When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path, using cost only to break ties (see RFC 2328).

  If there any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2 (RFC 2328), RFC 1583 should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code.
- **SPF Hold Time** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535 seconds; Default: 10 seconds)

  Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- **Area Numbers**[21] – The number of configured areas attached to this router.

Default Route Information –

- **Originate Default Route**[22] – Generates a default external route into an autonomous system. Note that the **AS Boundary Router** field must be enabled, and the **Advertise Default Route** field properly configured. (Default: Disabled)

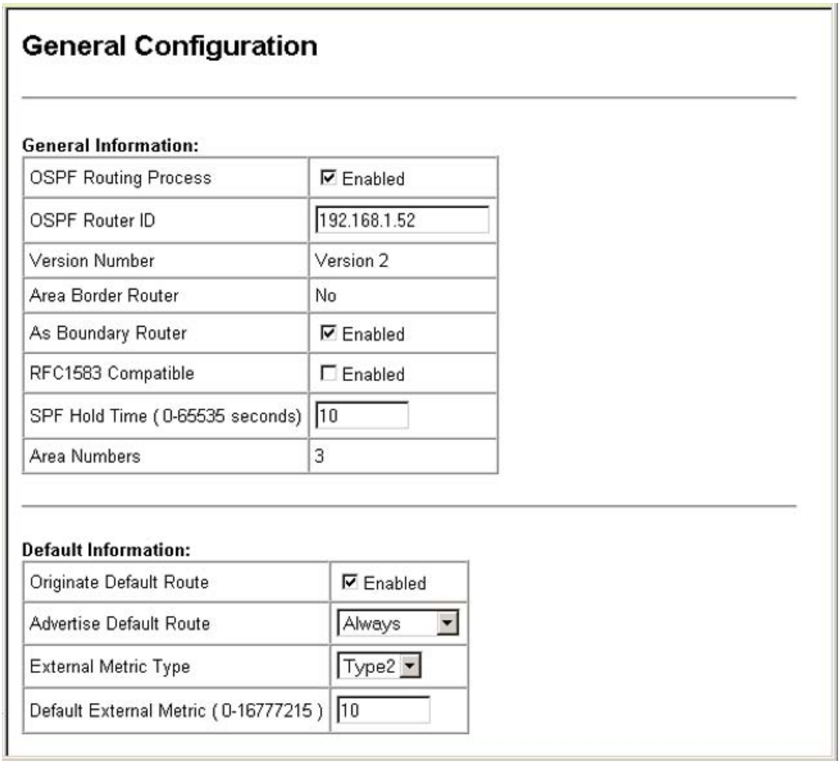
  When this feature is used to redistribute routes into a routing domain (that is, an Autonomous System), this router automatically becomes an Autonomous System Boundary Router (ASBR). This allows the router to exchange routing information with boundary routers in other autonomous systems to which it may be attached. If a router is functioning as an ASBR, then every other router in the autonomous system can learn about external routes from this device.

[22] CLI - These are configured with the **default-information originate** command (page 42-21).

- **Advertise Default Route**[22] – The router can advertise a default external route into the autonomous system (AS). (Options: NotAlways, Always; Default: NotAlways)
  - **Always** – The router will advertise itself as a default external route for the local AS, even if a default external route does not actually exist. (To define a default route, see “Configuring Static Routes” on page 19-21.)
  - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes through RIP or static routes, and such a route is known. (See “Redistributing External Routes” on page 20-35.)
- **External Metric Type**[22] – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)
- **Default External Metric**[22] – The Metric assigned to the default route. (Range: 1-65535; Default: 10)

  The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.

Web - Click Routing Protocol, OSPF, General Configuration. Enable OSPF, specify the Router ID, configure the other global parameters as required, and click Apply.



General Configuration

General Information:

OSPF Routing Process	☑ Enabled
OSPF Router ID	192.168.1.52
Version Number	Version 2
Area Border Router	No
As Boundary Router	☑ Enabled
RFC1583 Compatible	□ Enabled
SPF Hold Time (0-65535 seconds)	10
Area Numbers	3

Default Information:

Originate Default Route	☑ Enabled
Advertise Default Route	Always
External Metric Type	Type2
Default External Metric (0-16777215)	10

Figure 20-6   OSPF General Configuration

CLI - This example configures the router with the same settings as shown in the screen capture for the web interface.

```
Console(config)#router ospf                                          42-19
Console(config-router)#router-id 10.1.1.253                          42-20
Console(config-router)#no compatible rfc1583                         42-20
Console(config-router)#default-information originate always
  metric 10 metric-type 2                                            42-21
Console(config-router)#timers spf 10                                 42-22
Console(config-router)#
```

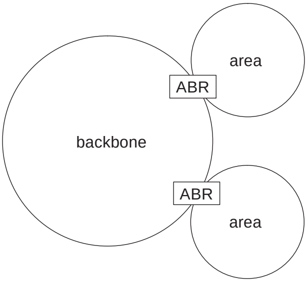
Configuring OSPF Areas

OSPF protocol broadcast messages (that is, Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

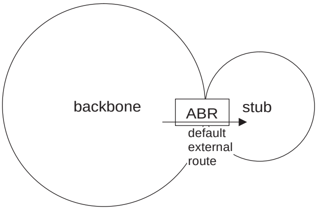
Use the Area Configuration screen to define an OSPF area and the interfaces that operate within this area. An autonomous system must be configured with a backbone area, designated by area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, you can configure an area to export a single summarized route that covers a broad range of network addresses within the area (page 20-23). To further reduce the amount of routes passed between areas, you can configure an area as a stub or a not-so-stubby area (NSSA).

Normal Area – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.



Stub – A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.

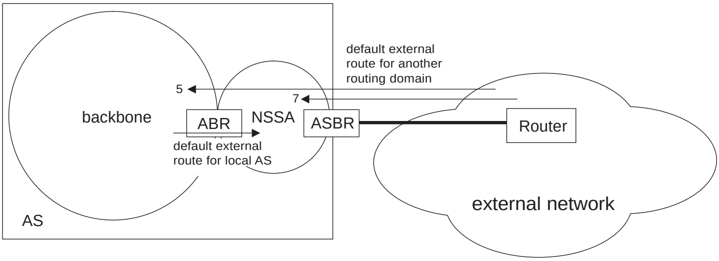


By default, a stub can only pass traffic to other areas in the autonomous system via the default external route. However, you also can configure an area border router to send Type 3 summary link advertisements into the stub about subnetworks located elsewhere in the autonomous system.

NSSA – A not-so-stubby area (NSSA) can be configured to control the use of default routes for Area Border Routers (ABRs) and Autonomous System Boundary Routers (ASBRs), or external routes learned from other routing domains and imported through an ABR.

An NSSA is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS) when the router is an ABR.

An NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by ABRs. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.



There are no external routes in an OSPF stub area, so routes cannot be redistributed from another protocol into a stub area. On the other hand, an NSSA allows external routes from another protocol to be redistributed into its own area, and then leaked to adjacent areas.

Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned via OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.

Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.

An NSSA can be used to simplify administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. OSPF can be easily extended to cover the remote connection by defining the area between the central router and the remote router as an NSSA.

Default Cost – This specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR).

Command Usage

- Before you create the backbone, a stub or NSSA, first specify the address range for the area using the Network Area Address Configuration screen (page 20-31).
- Stubs and NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- A stub or NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

Command Attributes

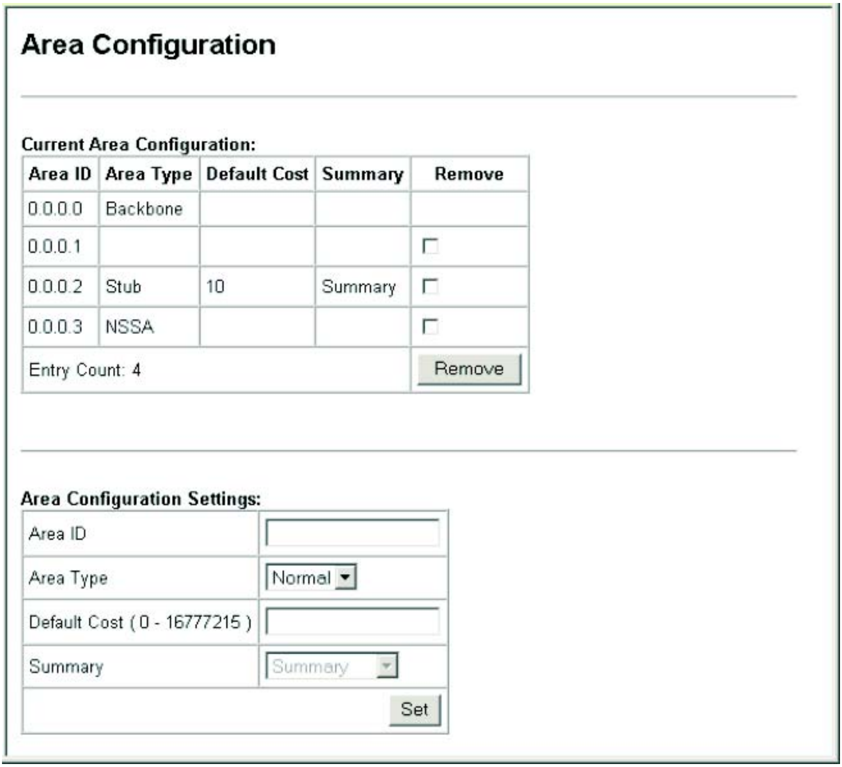
- **Area ID** – Identifier for an normal area, stub or NSSA. The area ID must be in the form of an IPv4 address.
- **Area Type** – Specifies a normal area, stub area, or not-so-stubby area (NSSA). Area ID 0.0.0.0 is set to the backbone by default. (Default: Normal area)
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 1)
  - Note that if you set the default cost to “0,” the router will not advertise a default route into the attached stub.
- **Summary** – Makes an ABR send a Type-3 summary link advertisement into a stub. (Default: Summary)

  A stub is designed to save routing table space by blocking Type-4 AS summary LSAs and Type 5 external LSAs. If you use the “NoSummary” option to also block Type-3 summary LSAs that advertise the default route for destinations external to the local area or the AS, the stub will become completely isolated.

  Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Area Configuration. Set any area to a stub or NSSA as required, specify the cost for the default summary route sent into a stub, and click Apply.



Area Configuration

Current Area Configuration:

Area ID	Area Type	Default Cost	Summary	Remove
0.0.0.0	Backbone			
0.0.0.1				□
0.0.0.2	Stub	10	Summary	□
0.0.0.3	NSSA			□
Entry Count: 4				Remove

Area Configuration Settings:

Area ID	
Area Type	Normal ▾
Default Cost (0 - 16777215)	
Summary	Summary ▾
	Set

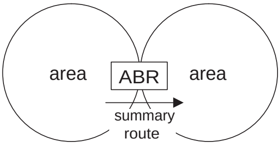
Figure 20-7 OSPF Area Configuration

CLI - This example configures area 0.0.0.1 as a normal area, area 0.0.0.2 as a stub, and area 0.0.0.3 as an NSSA. It also configures the router to propagate a default summary route into the stub and sets the cost for this default route to 10.

```
Console(config-router)#network 10.1.1.0 255.255.255.0 area 0.0.0.1   42-26
Console(config-router)#area 0.0.0.2 stub summary                     42-27
Console(config-router)#area 0.0.0.2 default-cost 10                  42-24
Console(config-router)#area 0.0.0.3 nssa                             42-28
Console(config-router)#end
```

```
Console#show ip ospf                                                        42-39
Routing Process with ID 192.168.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 3
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 40 times
Area 0.0.0.2 (STUB)
     Number of interfaces in this area is 1
     SPF algorithm executed 8 times
Area 0.0.0.3 (NSSA)
     Number of interfaces in this area is 1
     SPF algorithm executed 40 times
Console#
```

Configuring Area Ranges (Route Summarization for ABRs)



An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, you can configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

Command Usage

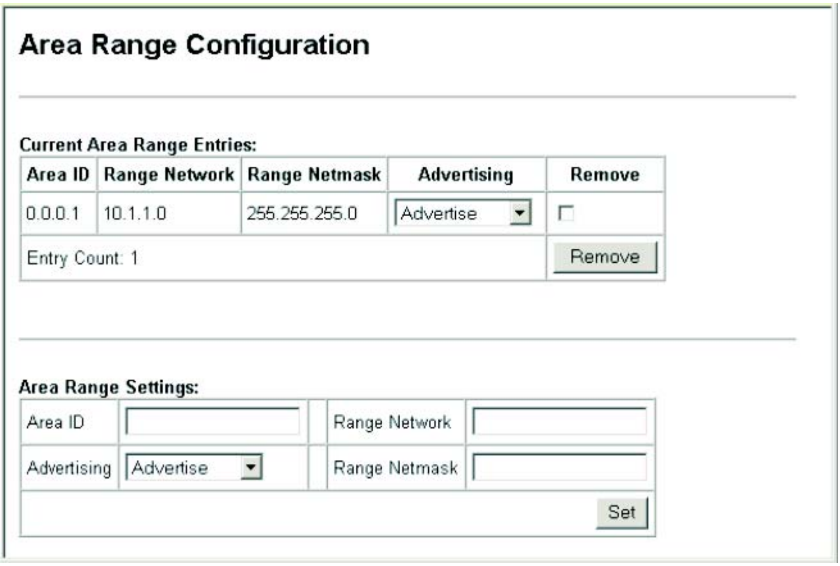
- Use the Area Range Configuration page to summarize intra-area routes, and advertise this information to other areas through Area Border Routers (ABRs). The summary route for an area is defined by an IP address and network mask. You therefore need to structure each area with a contiguous set of addresses so that all routes in the area fall within an easily specified range. If it is not possible to use one contiguous set of addresses, then the routes can be summarized for several area ranges.This router also supports Variable Length Subnet Masks (VLSMs), so you can summarize an address range on any bit boundary in a network address.
- To summarize the external LSAs imported into your autonomous system (i.e., local routing domain), use the Summary Address Configuration screen (page 20-33).

Command Attributes

- **Area ID** – Identifies an area for which the routes are summarized. (The area ID must be in the form of an IPv4 address.)
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route. If the routes are set to be advertised, the router will issue a Type 3 summary LSA for each specified address range. If the summary is not advertised, the specified routes remain hidden from the rest of the network. (Default: Advertise)

Note: This router supports up 64 summary routes for area ranges.

Web - Click Routing Protocol, OSPF, Area Range Configuration. Specify the area identifier, the base address and network mask, select whether or not to advertise the summary route to other areas, and then click Apply.



Area Range Configuration

Current Area Range Entries:

Area ID	Range Network	Range Netmask	Advertising	Remove
0.0.0.1	10.1.1.0	255.255.255.0	Advertise	□
Entry Count: 1				Remove

Area Range Settings:

Area ID		Range Network	
Advertising	Advertise	Range Netmask	
			Set

Figure 20-8 OSPF Range Configuration

CLI - This example summarizes all the routes for area 1. Note that the default for the **area range** command is to advertise the route summary. The configured summary route is shown in the list of information displayed for area 1.

```
Console(config-router)#area 0.0.0.1 range 10.1.1.0 255.255.255.0     42-23
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 0
     SPF algorithm executed 47 times
Area 0.0.0.1
     Number of interfaces in this area is 3
     SPF algorithm executed 14 times
     Area ranges are
        255.255.255.0/24  Active
Console#
```

Configuring OSPF Interfaces

You should specify a routing interface for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (i.e., one primary interface and one or more secondary interfaces), and then use the OSPF / Network Area Address Configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, you need to use the OSPF / Interface Configuration page to configure the interface-specific parameters used by OSPF to select the designated router, control the timing of link state advertisements, set the cost used to select preferred paths, and specify the method used to authenticate routing messages.

Field Attributes

OSPF Interface List

- **VLAN ID** – The VLAN to which an IP interface has been assigned.
- **Interface IP** – The IP interface associated with the selected VLAN.
- **Area ID** – The area to which this interface has been assigned.
- **Designated Router** – Designated router for this area.
- **Backup Designated Router** – Designated backup router for this area.
- **Entry Count** – The number of IP interfaces assigned to this VLAN.

Note: This router supports up 64 OSPF interfaces.

Detailed Interface Configuration

- **VLAN ID** – The VLAN corresponding to the selected interface.
- **Rtr Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)

  A designated router (DR) and backup designated router (BDR) is elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.

  The router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same priority, the router with the higher ID will be elected. You can set the priority to zero to prevent a router from being elected as a DR or BDR.

  If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

  Configure router priority for multi-access networks only and not for point-to-point networks.
- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1 second)

  LSAs have their age incremented by this delay before transmission. You should consider both the transmission and propagation delays for an interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.

If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, you can use the transmit delay to force the router to wait a specified interval between transmissions.

- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 5 seconds)

  A router will resend an LSA to a neighbor if it receives no acknowledgment after the specified retransmit interval. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

  Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

- **Hello Interval** – Sets the interval between sending hello packets on an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 10)

  Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

- **Rtr Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)

  The dead-interval is advertised in the router's hello packets. It must be a multiple of hello-interval and be the same for all routers on a specific network.

- **Cost** – Sets the cost of sending a protocol packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)

  The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.

  Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.

  This router uses a default cost of 1 for all ports. Therefore, if you install a 10 Gigabit module, you need to reset the cost for all of the 1 Gbps ports to a value greater than 1 to reflect the actual interface bandwidth.

- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple password, MD5; Default: None)

  Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password (or key). All neighboring routers on the same network with the same password will exchange routing data.

When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.

When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the prespecified target message digest.

Before specifying MD5 authentication, configure the message-digest key-id and key (see Message Digest Key-id).

The Authentication Key and Message Digest Key-id must be used consistently throughout the autonomous system. (Note that the Message Digest Key-id field is enabled only when MD5 authentication type is selected.)

- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)

  When plain-text or Message-Digest 5 (MD5) authentication is enabled as described in the preceding item, this password (key) is inserted into the OSPF header when routing protocol packets are originated by this device.

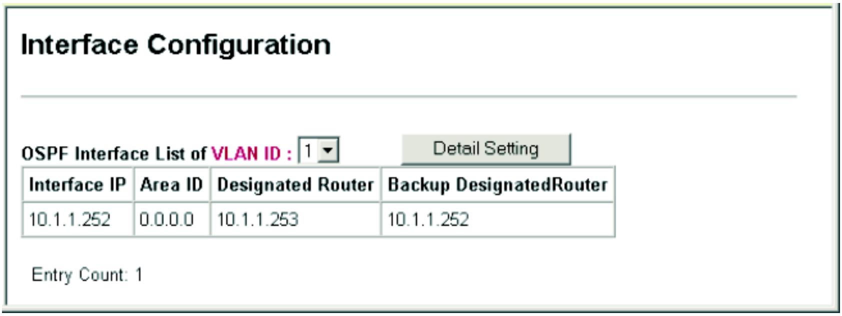
  A different password can be assigned to each network interface, but the password must be used consistently on all neighboring routers throughout a network (that is, autonomous system). All neighboring routers in the same network with the same password will exchange routing data.

- **Message Digest Key-id** – Assigns a key-id used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)

  Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.

  When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Web - Click Routing Protocol, OSPF, Interface Configuration. Select the required interface from the scroll-down box, and click Detailed Settings.



Interface Configuration

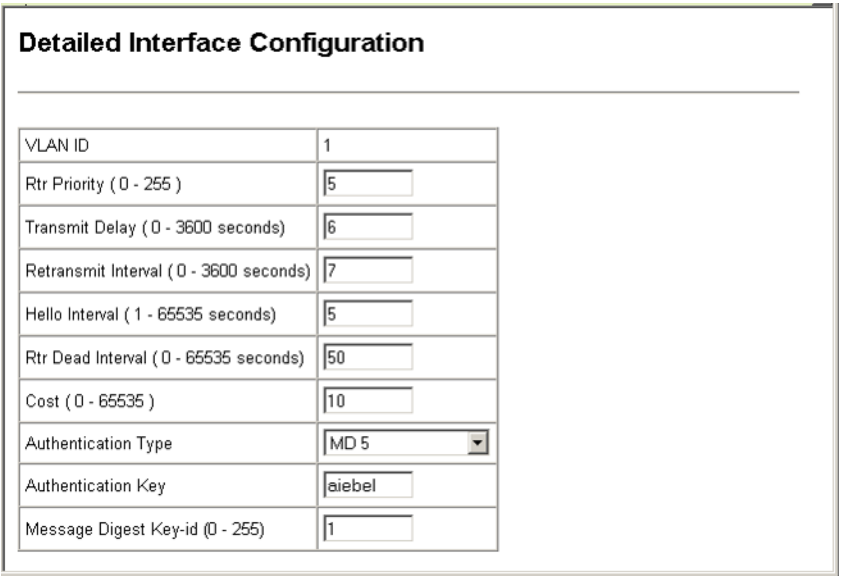
OSPF Interface List of VLAN ID : 1

Interface IP	Area ID	Designated Router	Backup DesignatedRouter
10.1.1.252	0.0.0.0	10.1.1.253	10.1.1.252

Entry Count: 1

Figure 20-9 OSPF Interface Configuration

Change any of the interface-specific protocol parameters, and then click Apply.



Detailed Interface Configuration

VLAN ID	1
Rtr Priority (0 - 255)	5
Transmit Delay (0 - 3600 seconds)	6
Retransmit Interval (0 - 3600 seconds)	7
Hello Interval (1 - 65535 seconds)	5
Rtr Dead Interval (0 - 65535 seconds)	50
Cost (0 - 65535)	10
Authentication Type	MD 5
Authentication Key	aiebel
Message Digest Key-id (0 - 255)	1

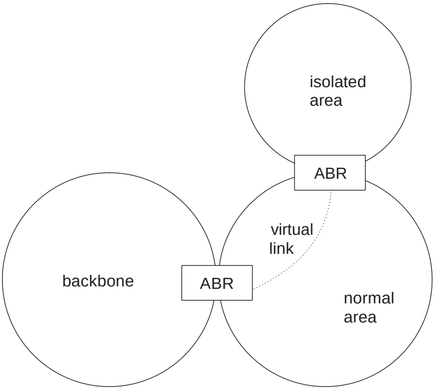
Figure 20-10 OSPF Interface Configuration - Detailed

CLI - This example configures the interface parameters for VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5                               42-37
Console(config-if)#ip ospf transmit-delay 6                         42-38
Console(config-if)#ip ospf retransmit-interval 7                    42-38
Console(config-if)#ip ospf hello-interval 5                         42-36
Console(config-if)#ip ospf dead-interval 50                         42-36
Console(config-if)#ip ospf cost 10                                  42-35
Console(config-if)#ip ospf authentication message-digest            42-32
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel          42-34
Console#
```

Configuring Virtual Links

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, you can configure a virtual link that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (i.e., transit area) to reach the backbone. To define this path, you must configure an ABR that serves as an endpoint connecting the isolated area to the common transit area, and specify a neighboring ABR as the other endpoint connecting the common transit area to the backbone itself. (Note that you cannot configure a virtual link that runs through a stub or NSSA area.)



Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

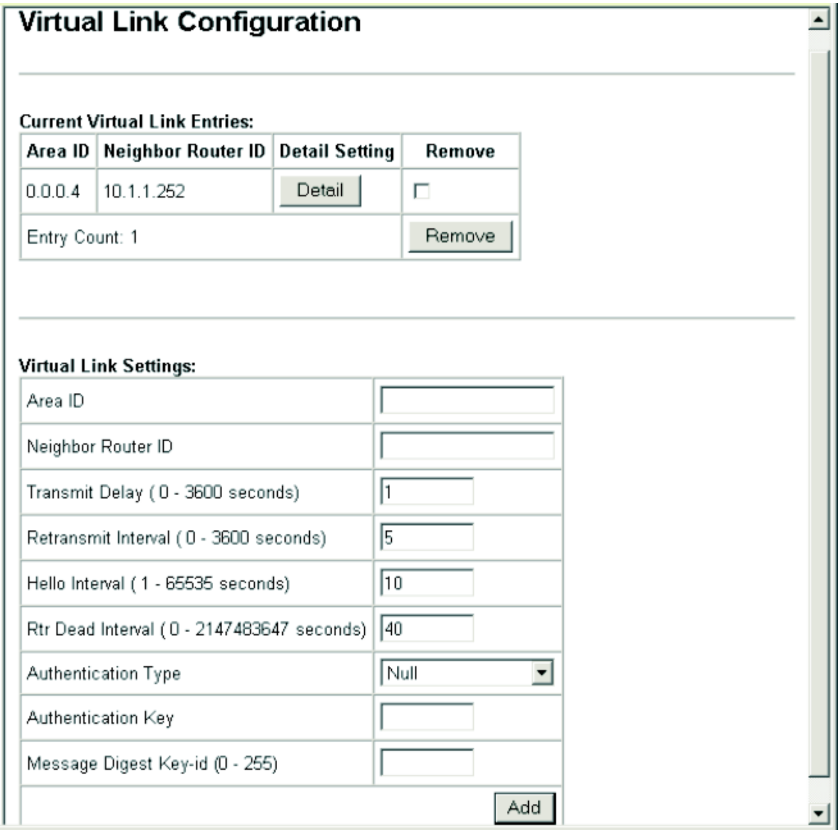
Command Attributes

- **Area ID** – Identifies the transit area for the virtual link. (The area ID must be in the form of an IPv4 address.)
- **Neighbor Router ID** – Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, it must be configured for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link. (Default: None)

The other items are described under “Configuring OSPF Interfaces,” page 20-25.

Note: This router supports up 64 virtual links.

Web - Click Routing Protocol, OSPF, Virtual Link Configuration. To create a new virtual link, specify the Area ID and Neighbor Router ID, configure the link attributes, and click Add. To modify the settings for an existing link, click the Detail button for the required entry, modify the link settings, and click Set.



Virtual Link Configuration

Current Virtual Link Entries:

Area ID	Neighbor Router ID	Detail Setting	Remove
0.0.0.4	10.1.1.252	Detail	□
Entry Count: 1			Remove

Virtual Link Settings:

Area ID	
Neighbor Router ID	
Transmit Delay (0 - 3600 seconds)	1
Retransmit Interval (0 - 3600 seconds)	5
Hello Interval (1 - 65535 seconds)	10
Rtr Dead Interval (0 - 2147483647 seconds)	40
Authentication Type	Null
Authentication Key	
Message Digest Key-id (0 - 255)	
	Add

Figure 20-11 OSPF Virtual Link Configuration

CLI - This example configures a virtual link from the ABR adjacent to area 0.0.0.4, through a transit area to the neighbor router 10.1.1.252 at the other end of the link which is adjacent to the backbone.

```
Console(config-router)#area 0.0.0.0 virtual-link 10.1.1.252         42-30
Console(config-router)#
```

Configuring Network Area Addresses

OSPF protocol broadcast messages (i.e., Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Command Usage

- Use the Network Area Address Configuration page to specify an Area ID and the corresponding network address range. Each area identifies a logical group of OSPF routers that actively exchange LSAs to ensure that they share an identical view of the network topology.
- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. The fixed value 0.0.0.0 is used as the Area ID for the backbone. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.
- An area initially configured via the Network Area Address Configuration page (other than the backbone) is set as a normal area (or transit area) by default. A normal area can send and receive external Link State Advertisements (LSAs). If necessary, you can use the Area Configuration page to configure an area as a stubby area that *cannot* send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area (page 20-19).
- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network (page 20-23).
- If an address range is overlapped with other network areas, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

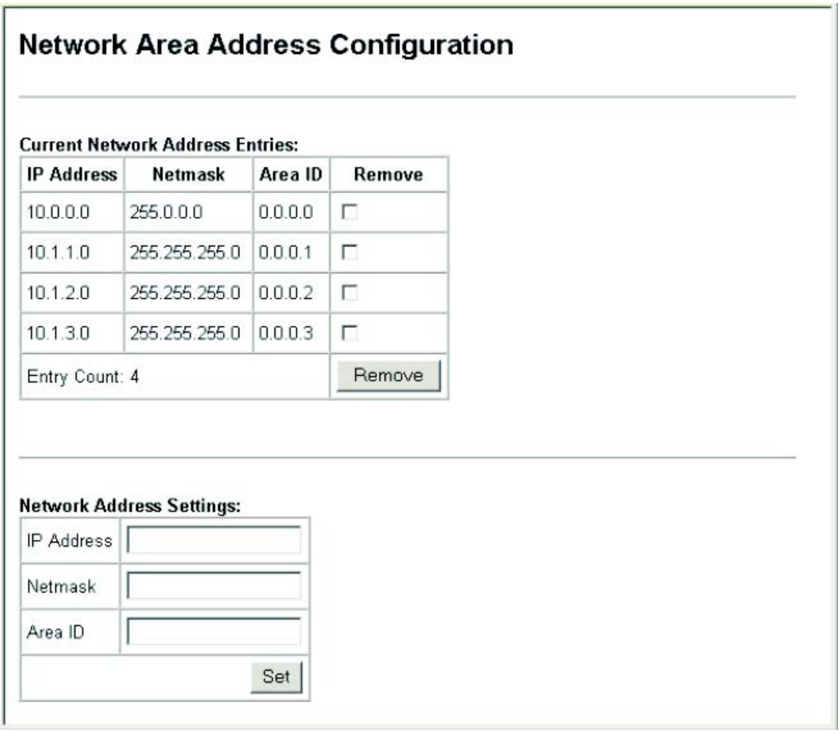
Command Attributes

- **IP Address** – Address of the interfaces to add to the area.
- **Netmask** – Network mask of the address range to add to the area.
- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IPv4 address.)

  Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Network Area Address Configuration. Configure a backbone area that is contiguous with all the other areas in your network, configure an area for all of the other OSPF interfaces, then click Apply.



Network Area Address Configuration

Current Network Address Entries:

IP Address	Netmask	Area ID	Remove
10.0.0.0	255.0.0.0	0.0.0.0	□
10.1.1.0	255.255.255.0	0.0.0.1	□
10.1.2.0	255.255.255.0	0.0.0.2	□
10.1.3.0	255.255.255.0	0.0.0.3	□
Entry Count: 4			Remove

Network Address Settings:

IP Address	
Netmask	
Area ID	
	Set

Figure 20-12 OSPF Network Area Address Configuration

CLI - This example configures the backbone area and one transit area.

```
Console(config-router)#network 10.0.0.0 255.0.0.0 area 0.0.0.0     42-26
Console(config-router)#network 10.1.1.0 255.255.255.0 area 0.0.0.1
Console(config-router)#end
Console#show ip ospf                                                42-39
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 8 times
Area 0.0.0.1
     Number of interfaces in this area is 1
     SPF algorithm executed 5 times
Area 0.0.0.2 (STUB)
     Number of interfaces in this area is 1
     SPF algorithm executed 13 times
Area 0.0.0.3 (NSSA)
     Number of interfaces in this area is 1
     SPF algorithm executed 12 times
Console#
```

Configuring Summary Addresses (for External AS Routes)

Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA. An Autonomous System Boundary Router (ASBR) can be configured to redistribute routes learned from other protocols into all attached autonomous systems. (See “Redistributing External Routes” on page 20-35.)

To reduce the amount of external LSAs sent to other autonomous systems, you can configure the router to advertise an aggregate route that consolidates a broad range of external addresses. This helps both to decrease the number of external LSAs advertised and the size of the OSPF link state database.

Command Usage

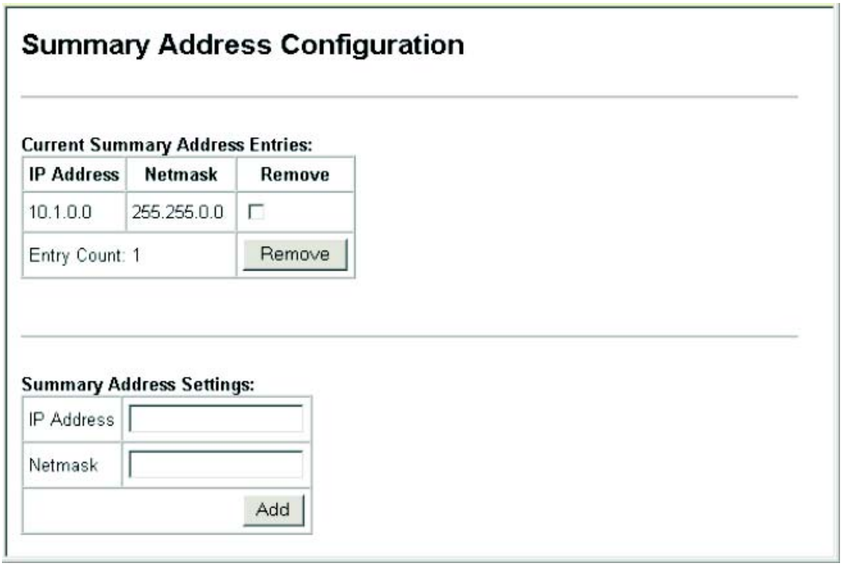
- If you are not sure what address ranges to consolidate, first enable external route redistribution via the Redistribute Configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.
- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 20-23).

Command Attributes

- **IP Address** – Summary address covering a range of addresses.
- **Netmask** – Network mask for the summary route.

Note: This router supports up 16 Type-5 summary routes.

Web - Click Routing Protocol, OSPF, Summary Address Configuration. Specify the base address and network mask, then click Add.



Summary Address Configuration

Current Summary Address Entries:

IP Address	Netmask	Remove
10.1.0.0	255.255.0.0	□
Entry Count: 1		Remove

Summary Address Settings:

IP Address	
Netmask	
	Add

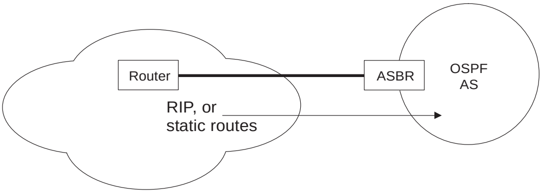
Figure 20-13 OSPF Summary Address Configuration

CLI - This example This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0      42-24
Console(config-router)#
```

Redistributing External Routes

You can configure this router to import external routing information from other routing protocols or static routes into the autonomous system, and to generate AS-external-LSAs.



Command Usage

- This router supports redistribution for entries learned through RIP, and static routes.
- When you redistribute external routes into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been manually configured as an ASBR via the General Configuration screen, but redistribution is not enabled, the router will only generate a “default” external route into the AS if it has been configured to “always” advertise a default route even if an external route does not actually exist (page 20-15).

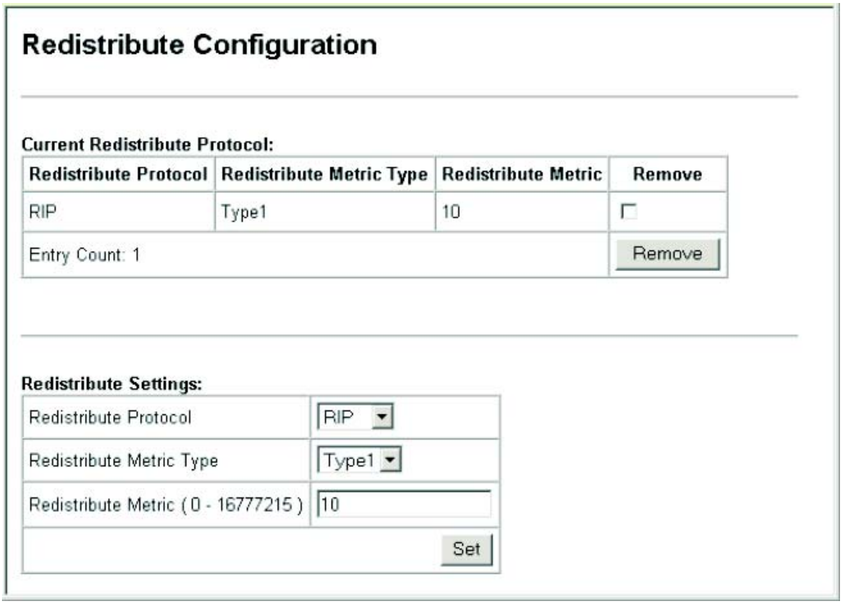
Command Attributes

- **Redistribute Protocol** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)
- **Redistribute Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)

  Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) through External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.
- **Redistribute Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)

  The metric value specified for redistributed routes supersedes the Default External Metric specified in the OSPF / General Configuration screen (page 20-15).

Web - Click Routing Protocol, OSPF, Redistribute. Specify the protocol type to import, the metric type and path cost, then click Add.



Redistribute Configuration

Current Redistribute Protocol:

Redistribute Protocol	Redistribute Metric Type	Redistribute Metric	Remove
RIP	Type1	10	□
Entry Count: 1			Remove

Redistribute Settings:

Redistribute Protocol	RIP
Redistribute Metric Type	Type1
Redistribute Metric (0 - 16777215)	10
	Set

Figure 20-14 OSPF Redistribute Configuration

CLI - This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1                  42-25
Console(config-router)#
```

Configuring NSSA Settings

Use the OSPF / NSSA Settings page to configure a not-so-stubby area (NSSA), and to control the use of default routes for ABRs and ASBRs, or external routes learned from other routing domains and imported through an ABR. (For a detailed description of NSSA areas, refer to “Configuring OSPF Areas” on page 20-19.)

Command Attributes

- **Area ID** – Identifier for an not-so-stubby area (NSSA). The area ID must be in the form of an IPv4 address.
- **Default Information Originate** – An NSSA ASBR originates and floods Type-7 external LSAs throughout its area for known network destination outside of the AS. However, you can also configure an NSSA ASBR to generate a Type-7 “default” route to areas outside of the AS, or an NSSA ABR to generate a Type-7 “default” route to other areas within the AS. (Default: Disabled)

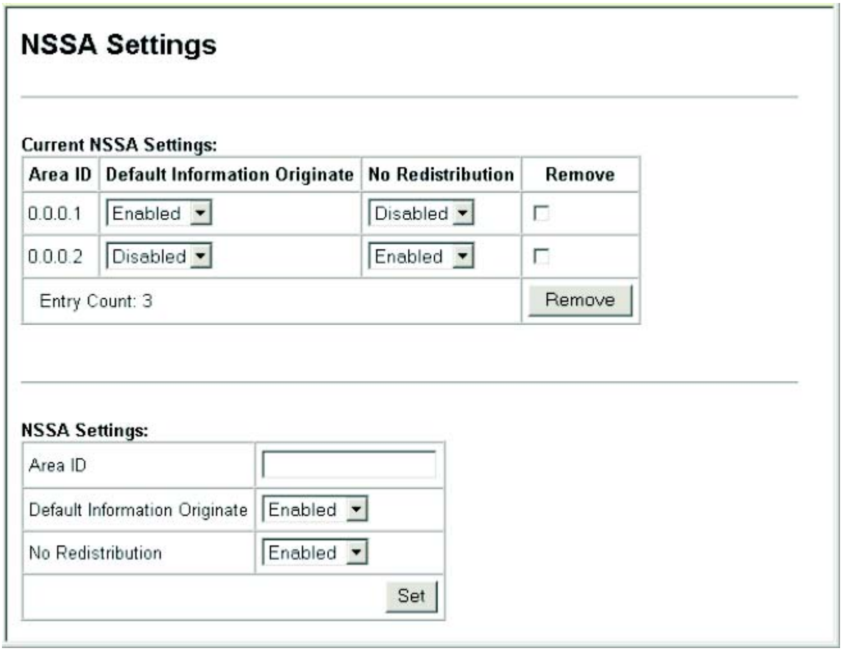
  An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the Originate Default

Information option. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using this option.

- **No Redistribution** – Use this option when the router is an NSSA Area Border Router (ABR) and routes only need to be imported into normal areas (page 20-35), but not into the NSSA. In other words, redistribution should be disabled to prevent the NSSA ABR from advertising external routing information (learned through routers in other areas) into the NSSA. (Default: Enabled)

Note: This router supports up 16 areas, either normal transit areas, stubs, or NSSAs.

Web - Click Routing Protocol, OSPF, NSSA Settings. Create a new NSSA or modify the routing behavior for an existing NSSA, and click Apply.



NSSA Settings

Current NSSA Settings:

Area ID	Default Information Originate	No Redistribution	Remove
0.0.0.1	Enabled	Disabled	□
0.0.0.2	Disabled	Enabled	□
Entry Count: 3			Remove

NSSA Settings:

Area ID	
Default Information Originate	Enabled
No Redistribution	Enabled
	Set

Figure 20-15 OSPF NSSA Settings

CLI - This example configures area 0.0.0.1 as a stub and sets the cost for the default summary route to 10.

```
Console(config-router)#area 0.0.0.1 nssa
 default-information originate                               42-21
Console(config-router)#area 0.0.0.2 nssa no-redistribution   42-28
Console(config-router)#
```

Displaying Link State Database Information

OSPF routers advertise routes using Link State Advertisements (LSAs). The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. You can show information about different LSAs stored in this router's database, which may include any of the following types:

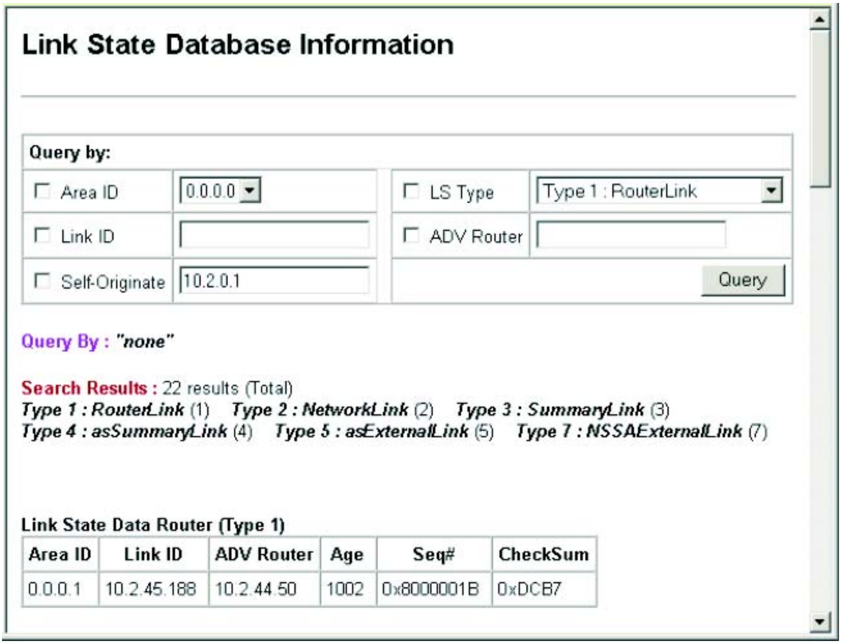
- Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.
- Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.
- Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.
- AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).
- AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.
- NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

Command Attributes

- **Area ID** – Area defined for which you want to view LSA information. (This item must be entered in the form of an IPv4 address.)
- **Link ID** – The network portion described by an LSA. The Link ID should be:
  - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)
  - A Router ID for Router, Network, and Type 4 AS Summary LSAs.
- **Self-Originate** – Shows LSAs originated by this router.
- **LS Type** – LSA Type (Options: Type 1-5, 7). See the preceding description.
- **Adv Router** – IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- **Age**[23] – Age of LSA (in seconds).
- **Seq**[23] – Sequence number of LSA (used to detect older duplicate LSAs).
- **CheckSum**[23] – Checksum of the complete contents of the LSA.

[23] These items are read only.

Web - Click Routing Protocol, OSPF, Link State Database Information. Specify parameters for the LSAs you want to display, then click Query.



Link State Database Information

Query by:

□ Area ID	0.0.0.0	□ LS Type	Type 1 : RouterLink
□ Link ID		□ ADV Router	
□ Self-Originate	10.2.0.1		Query

Query By : "none"

Search Results : 22 results (Total)
Type 1 : RouterLink (1) *Type 2 : NetworkLink* (2) *Type 3 : SummaryLink* (3)
Type 4 : asSummaryLink (4) *Type 5 : asExternalLink* (5) *Type 7 : NSSAExternalLink* (7)

Link State Data Router (Type 1)

Area ID	Link ID	ADV Router	Age	Seq#	CheckSum
0.0.0.1	10.2.45.188	10.2.44.50	1002	0x8000001B	0xDCB7

Figure 20-16 OSPF Link State Database Information

CLI - The CLI provides a wider selection of display options for viewing the Link State Database. See “show ip ospf database” on page 42-41.

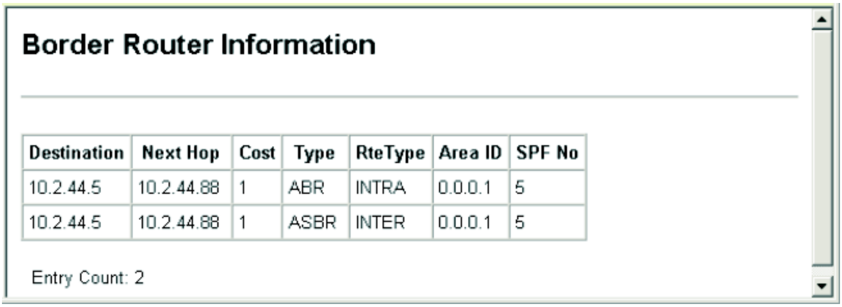
Displaying Information on Border Routers

You can display entries in the local routing table for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) known by this device.

Field Attributes

- **Destination** – Identifier for the destination router.
- **Next Hop** – IP address of the next hop toward the destination.
- **Cost** – Link metric for this route.
- **Type** – Router type of the destination; either ABR, ASBR or both.
- **Rte Type** – Route type; either intra-area or interarea route (INTRA or INTER).
- **Area** – The area from which this route was learned.
- **SPF No** – The number of times the shortest path first algorithm has been executed for this route.

Web - Click Routing Protocol, OSPF, Border Router Information.



Border Router Information

Destination	Next Hop	Cost	Type	RteType	Area ID	SPF No
10.2.44.5	10.2.44.88	1	ABR	INTRA	0.0.0.1	5
10.2.44.5	10.2.44.88	1	ASBR	INTER	0.0.0.1	5

Entry Count: 2

Figure 20-17 OSPF Border Router Information

CLI - This example shows one router that serves as both the ABR for the local area and the ASBR for the autonomous system.

```
Console#show ip ospf border-routers                                      42-40

  Destination       Next Hop       Cost    Type  RteType       Area          SPF No
--------------- --------------- ------ ----- -------- --------------- -------
     10.2.44.5      10.2.44.88       1    ABR     INTRA          0.0.0.1        5
     10.2.44.5      10.2.44.88       1    ASBR    INTER          0.0.0.1        5
Console#
```

Displaying Information on Neighbor Routers

You can display about neighboring routers on each interface within an OSPF area.

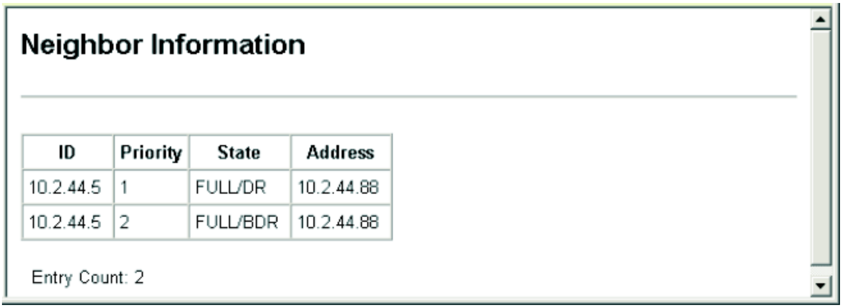
Field Attributes

- **ID** – Neighbor’s router ID.
- **Priority** – Neighbor’s router priority.
- **State** – OSPF state and identification flag.

  States include:
  - Down – Connection down
  - Attempt – Connection down, but attempting contact (non-broadcast networks)
  - Init – Have received Hello packet, but communications not yet established
  - Two-way – Bidirectional communications established
  - ExStart – Initializing adjacency between neighbors
  - Exchange – Database descriptions being exchanged
  - Loading – LSA databases being exchanged
  - Full – Neighboring routers now fully adjacent

  Identification flags include:
  - D – Dynamic neighbor
  - S – Static neighbor
  - DR – Designated router
  - BDR – Backup designated router
- **Address** – IP address of this interface.

Web - Click Routing Protocol, OSPF, Neighbor Information.



Neighbor Information

ID	Priority	State	Address
10.2.44.5	1	FULL/DR	10.2.44.88
10.2.44.5	2	FULL/BDR	10.2.44.88

Entry Count: 2

Figure 20-18 OSPF Neighbor Information

CLI - This shows a designated router and backup designated router as neighbors.

```
Console#show ip ospf neighbor                                          42-50

      ID           Pri        State            Address
--------------- ------ ---------------- ---------------
      10.2.44.5      1          FULL/DR       10.2.44.88
      10.2.44.6      2         FULL/BDR       10.2.44.88

Console#
```

Section III:Command Line Interface

This section provides a detailed description of the Command Line Interface, along with examples for all of the commands.

Chapter 21: Overview of the Command Line Interface

This chapter describes how to use the Command Line Interface (CLI).

Note: You can only access the console interface through the Master unit in the stack.

Using the Command Line Interface

Accessing the CLI

When accessing the management interface for the switch over a direct connection to the server’s console port, or via a Telnet connection, the switch can be managed by entering command keywords and parameters at the prompt. Using the switch's command-line interface (CLI) is very similar to entering commands on a UNIX system.

Console Connection

To access the switch through the console port, perform these steps:

1. At the console prompt, enter the user name and password. (The default user names are “admin” and “guest” with corresponding passwords of “admin” and “guest.”) When the administrator user name and password is entered, the CLI displays the “Console#” prompt and enters privileged access mode (i.e., Privileged Exec). But when the guest user name and password is entered, the CLI displays the “Console>” prompt and enters normal access mode (i.e., Normal Exec).

2. Enter the necessary commands to complete your desired tasks.

3. When finished, exit the session with the “quit” or “exit” command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

  CLI session with the 24/48 L3 GE Switch is opened.

  To end the CLI session, enter [Exit].

Console#
```

Telnet Connection

Telnet operates over the IP transport protocol. In this environment, your management station and any network device you want to manage over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion.

For example, the IP address assigned to this switch, 10.1.0.1, with subnet mask 255.255.255.0, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for this switch is obtained via DHCP by default.

To access the stack through a Telnet session, you must first set the IP address for the Master unit, and set the default gateway if you are managing the switch from a different IP subnet. For example,

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.254 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

If your corporate network is connected to another network outside your office or to the Internet, you need to apply for a registered IP address. However, if you are attached to an isolated network, then you can use any IP address that matches the network segment to which you are attached.

After you configure the switch with an IP address, you can open a Telnet session by performing these steps:

1. From the remote host, enter the Telnet command and the IP address of the device you want to access.
2. At the prompt, enter the user name and system password. The CLI will display the “Vty-*n*#” prompt for the administrator to show that you are using privileged access mode (i.e., Privileged Exec), or “Vty-*n*>” for the guest to show that you are using normal access mode (i.e., Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete your desired tasks.
4. When finished, exit the session with the “quit” or “exit” command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

  CLI session with the 24/48 L3 GE Switch is opened.

  To end the CLI session, enter [Exit].

Vty-0#
```

Note: You can open up to four sessions to the device via Telnet.

Entering Commands

This section describes how to enter CLI commands.

Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command “show interfaces status ethernet 1/5,” **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit/port.

You can enter commands as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enable Privileged Exec command mode, and display the startup configuration, enter:

  ```
  Console>enable
  Console#show startup-config
  ```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

  ```
  Console(config)#username admin password 0 smith
  ```

Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command “configure” can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

Command Completion

If you terminate input with a Tab key, the CLI will print the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab will result in printing the command up to “**logging**.”

Getting Help on Commands

You can display a brief description of the help system by entering the **help** command. You can also display command syntax by using the “?” character to list keywords or parameters.

Showing Commands

If you enter a “?” at the command prompt, the system will display the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, DHCP, Interface, Line, Router, VLAN Database, or MSTP). You can also display a list of valid keywords for a specific command. For example, the command “**show ?**” displays a list of possible show commands:

```
Console#show ?
  access-group       Access groups
  access-list        Access lists
  arp                Information of ARP cache
  bridge-ext         Bridge extend information
  calendar           Date information
  class-map          Display class maps
  clock
  dns                DNS information
  dot1q-tunnel       dot1q-tunnel
  dot1x              Show 802.1x content
  garp                GARP property
  gvrp                  Show GARP information of interface
  history              Information of history
  hosts               Host information
  interfaces           Information of interfaces
  ip                  IP information
  ipv6                IPv6 information
  lacp                Show LACP statistic
  line                 TTY line information
  lldp               LLDP
  log                 Login records
  logging               Show the contents of logging buffers
  mac                 MAC access lists
  mac-address-table  Set configuration of the address table
  management           Show management IP filter
  map                 Map priority
  policy-map          Display policy maps
  port                 Characteristics of the port
  port-channel        Port channel
  protocol-vlan        Protocol-VLAN information
  public-key           Show information of public key
  pvlan                Information of private VLAN
  queue                Information of priority queue
  radius-server        RADIUS server information
  rip                RIP
  router             Router
  running-config        The system configuration of running
  snmp                SNMP statistics
  sntp               SNTP
  spanning-tree        Specify spanning-tree
  ssh                 Secure shell
  startup-config        The system configuration of starting up
  system               Information of system
  tacacs-server        Login by TACACS server
  tech-support         Technical information
  users                 Display information about terminal lines
  version               System hardware and software status
  vlan                 Switch VLAN Virtual Interface
  vrrp                Show vrrp
Console#show
```

The command “**show interfaces ?**” will display the following information:

```
Console#show interfaces ?
  counters         Information of interfaces counters
  protocol-vlan  Protocol-vlan information
  status           Information of interfaces status
  switchport       Information of interfaces switchport
Console#
```

Partial Keyword Lookup

If you terminate a partial keyword with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example “**s?**” shows all the keywords starting with “s.”

```
Console#show s?
snmp          sntp           spanning-tree   ssh            startup-config
system
Console#sh s
```

Negating the Effect of Commands

For many configuration commands you can enter the prefix keyword “**no**” to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command will log system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

Using Command History

The CLI maintains a history of commands that have been entered. You can scroll back through the history of commands by pressing the up arrow key. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. You can always enter a question mark “**?**” at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in the following table:

Table 21-1 General Command Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map DHCP Interface Line Multiple Spanning Tree Policy Map Router VLAN Database

* You must be in Privileged Exec mode to access the Global configuration mode.
You must be in Global Configuration mode to access any of the other configuration modes.

Exec Commands

When you open a new console session on the switch with the user name and password “guest,” the system enters the Normal Exec command mode (or guest mode), displaying the “Console>” command prompt. Only a limited number of the commands are available in this mode. You can access all commands only from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a new console session with the user name and password “admin.” The system will now display the “Console#” command prompt. You can also enter Privileged Exec mode from within Normal Exec mode, by entering the **enable** command, followed by the privileged level password “super” (page 22-1).

To enter Privileged Exec mode, enter the following user names and passwords:

```
Username: admin
Password: [admin login password]

  CLI session with the 24/48 L3 GE Switch is opened.
  To end the CLI session, enter [Exit].

Console#
```

```
Username: guest
Password: [guest login password]

  CLI session with the 24/48 L3 GE Switch is opened.
  To end the CLI session, enter [Exit].

Console>enable
Password: [privileged level password]
Console#
```

Configuration Commands

Configuration commands are privileged level commands used to modify switch settings. These commands modify the running configuration only and are not saved when the switch is rebooted. To store the running configuration in non-volatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- DHCP Configuration - These commands are used to configure the DHCP server.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include command such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- Router Configuration - These commands configure global settings for unicast routing protocols.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt will change to “Console(config)#” which gives you access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 21-2 Configuration Command Modes

Mode	Command	Prompt	Page
Line	line {console | vty}	Console(config-line)	23-17

Access Control List	access-list ip standard
	access-list ip extended
	access-list mac
	access-list ipv6 standard
	access-list ipv6 extended
		Console(config-std-acl)
		Console(config-ext-acl)
		Console(config-mac-acl)
		Console(config-std-ipv6-acl)
		Console(config-ext-ipv6-acl)
			26-2
			26-2
			26-12
			26-7
			26-7

Class Map	class map	Console(config-cmap)	36-2
DHCP	ip dhcp pool	Console(config-dhcp)	39-6
Interface	interface {ethernet *port* | port-channel *id*| vlan *id*}	Console(config-if)	27-1
MSTP	spanning-tree mst-configuration	Console(config-mstp)	33-7
Policy Map	policy map	Console(config-pmap)	36-5
Router	router {rip | ospf}	Console(config-router)	42-6 42-19
VLAN	vlan database	Console(config-vlan)	34-5

For example, you can use the following commands to enter interface configuration mode, and then return to Privileged Exec mode

```
Console(config)#interface ethernet 1/5
:
Console(config-if)#exit
Console(config)#
```

Command Line Processing

Commands are not case sensitive. You can abbreviate commands and parameters as long as they contain enough letters to differentiate them from any other currently available commands or parameters. You can use the Tab key to complete partial commands, or enter a partial command followed by the “?” character to display a list of possible matches. You can also use the following editing keystrokes for command-line processing:

Table 21-3 Keystroke Commands

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.
Ctrl-P	Enters the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes from the cursor to the beginning of the line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

Command Groups

The system commands can be broken down into the functional groups shown below.

Table 21-4 Command Group Index

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	22-1
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, and the system clock	23-1
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	24-1
User Authentication	Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses	25-1
Access Control List	Provides filtering for IPv4 frames (based on address, protocol, TCP/UDP port number or TCP control code), IPv6 frames (based on destination address, next header type, or flow label), or non-IP frames (based on MAC address or Ethernet type)	26-1
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	27-1
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	28-1
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	29-1
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	30-1
Address Table	Configures the address table for filtering specified addresses, displays current entries, clears the table, or sets the aging time	31-1
Spanning Tree	Configures Spanning Tree settings for the switch	33-1
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs and protocol VLANs	34-1
Class of Service	Sets port priority for untagged frames, selects strict priority or weighted round robin, relative weight for each priority queue, also sets priority for TCP/UDP traffic types, IP precedence, and DSCP	35-1
Quality of Service	Configures Differentiated Services	36-1
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	37-1
Domain Name Service	Configures DNS services.	38-1
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	39-1
IP Interface	Configures IP address for the switch interfaces; also configures ARP parameters and static entries	41-1
IP Routing	Configures static and dynamic unicast routing	42-1
Router Redundancy	Configures router redundancy to create primary and backup routers	40-1

The access mode shown in the following tables is indicated by these abbreviations:

ACL (Access Control List Configuration)

CM (Class Map Configuration)

DC (DHCP Server Configuration)

GC (Global Configuration)

IC (Interface Configuration)

LC (Line Configuration)

MST (Multiple Spanning Tree)

NE (Normal Exec)

PE (Privileged Exec)

PM (Policy Map Configuration)

RC (Router Configuration)

VC (VLAN Database Configuration)

Chapter 22: General Commands

These commands are used to control the command access mode, configuration mode, and other basic functions.

Table 22-1 General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	22-1
disable	Returns to normal mode from privileged mode	PE	22-2
configure	Activates global configuration mode	PE	22-2
show history	Shows the command history buffer	NE, PE	22-3
reload	Restarts the system	PE	22-4
prompt	Customizes the CLI prompt	GC	22-4
end	Returns to Privileged Exec mode	any config. mode	22-4
exit	Returns to the previous configuration mode, or exits the CLI	any	22-5
quit	Exits a CLI session	NE, PE	22-5
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

enable

This command activates Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See “Understanding Command Modes” on page 21-6.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- “super” is the default password required to change the command mode from Normal Exec to Privileged Exec. (To set this password, see the **enable password** command on page 25-3.)

- The “#” character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console>enable
Password: [privileged level password]
Console#
```

Related Commands

disable (22-2)
enable password (25-3)

disable

This command returns to Normal Exec mode from privileged mode. In normal access mode, you can only display basic information on the switch's configuration or Ethernet statistics. To gain access to all commands, you must use the privileged mode. See “Understanding Command Modes” on page 21-6.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The “>” character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable
Console>
```

Related Commands

enable (22-1)

configure

This command activates Global Configuration mode. You must enter this mode to modify any settings on the switch. You must also enter Global Configuration mode prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration. See “Understanding Command Modes” on page 21-6.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure
Console(config)#
```

Related Commands

end (22-4)

show history

This command shows the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and
10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when you are in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when you are in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

reload

This command restarts the system.

Note: When the system is restarted, it will always run the Power-On Self-Test. It will also retain all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the switch:

```
Console#reload
System will be restarted, continue <y/n>? y
```

prompt

This command customizes the CLI prompt. Use the **no** form to restore the default prompt.

Syntax

prompt *string*
no prompt

string - Any alphanumeric string to use for the CLI prompt. (Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt RD2
RD2(config)#
```

end

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration.

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end
Console#
```

exit

This command returns to the previous configuration mode or exits the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session
User Access Verification

Username:
```

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit

Press ENTER to start session

User Access Verification

Username:
```

Chapter 23: System Management Commands

These commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 23-1 System Management Commands

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies this switch	23-1
System Status	Displays system configuration, active managers, and version information	23-3
Frame Size	Enables support for jumbo frames	23-9
File Management	Manages code image or switch configuration files	23-10
Line	Sets communication parameters for the serial port, including baud rate and console time-out	23-17
Event Logging	Controls logging of error messages	23-26
SMTP Alerts	Configures SMTP email alerts	23-32
Time (System Clock)	Sets the system clock automatically via NTP/SNTP server or manually	23-35

Device Designation Commands

This section describes commands used to configure information that uniquely identifies the switch.

Table 23-2 Device Designation Commands

Command	Function	Mode	Page
hostname	Specifies the host name for the switch	GC	23-1
snmp-server contact	Sets the system contact string	GC	24-4
snmp-server location	Sets the system location string	GC	24-4
switch renumber	Renumbers stack units	PE	23-2

hostname

This command specifies or modifies the host name for this device. Use the **no** form to restore the default host name.

Syntax

hostname *name*
no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname RD#1
Console(config)#
```

switch renumber

This command resets the switch unit identification numbers in the stack. All stack members are numbered sequentially starting from the top unit for a non-loop stack, or starting from the Master unit for a looped stack.

Syntax

switch all renumber

Default Setting

- For non-loop stacking, the top unit is unit 1.
- For loop stacking, the master unit is unit 1.

Command Mode

Global Configuration

Example

This example shows how to renumber all units.

```
Console#switch all renumber
Console#
```

System Status Commands

This section describes commands used to display system information.

Table 23-3 System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	23-3
show running-config	Displays the configuration data currently in use	PE	23-5
show system	Displays system information	NE, PE	23-7
show users	Shows a l active console and Telnet sessions, including user name, idle time, and IP address of Telnet clients	NE, PE	23-8
show version	Displays version information for the system	NE, PE	23-8

show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for each switch in the stack
  - SNTP server settings
  - SNMP community strings
  - Users (names and access levels)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show startup-config
building startup-config, please wait.....
!<stackingDB>00000000000000000</stackingDB>
!<stackingMac>01_00-20-1a-df-9c-a0_00</stackingMac>
!<stackingMac>02_00-20-1a-df-9e-c0_01</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
phymap 00-20-1a-df-9c-a0 00-20-1a-df-9e-c0 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community public ro
snmp-server community private rw!
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree MST configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
:
interface vlan 1
 ip address dhcp
!
no map IP precedence
no map IP DSCP
!
line console
!
line VTY
!
end

Console#
```

Related Commands

show running-config (23-5)

show running-config

This command displays the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by "!" symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
  - MAC address for each switch in the stack
  - SNTP server settings
  - SNMP community strings
  - Users (names, access levels, and encrypted passwords)
  - VLAN database (VLAN ID, name and state)
  - VLAN configuration settings for each interface
  - Multiple spanning tree instances (name and interfaces)
  - IP address configured for VLANs
  - Layer 4 precedence settings
  - Routing protocol configuration settings
  - Spanning tree settings
  - Any configured settings for the console port and Telnet

Example

```
Console#show running-config
building running-config, please wait.....
!<stackingDB>0000000000000000</stackingDB>
!<stackingMac>01_00-30-f1-d4-73-a0_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!<stackingMac>00_00-00-00-00-00-00_00</stackingMac>
!
phymap 00-30-f1-d4-73-a0 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00 00-00-00-00-00-00
00-00-00-00-00-00

!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
snmp-server community private rw
snmp-server community public ro
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
vlan database
 vlan 1 name DefaultVlan media ethernet state active
!
spanning-tree MST-configuration
!
interface ethernet 1/1
 switchport allowed vlan add 1 untagged
 switchport native vlan 1
:
interface vlan 1
 IP address DHCP
!
no map IP precedence
no map IP DSCP
!
line console
line vty
!
end
Console#
```

Related Commands

show startup-config (23-3)

show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to “Displaying System Information” on page 4-1.
- The POST results should all display “PASS.” If any POST test indicates “FAIL,” contact your distributor for assistance.

Example

```
Console#show system
System Description: 24/48 port 10/100/1000 Stackable Managed Switch
 with 2 X 10G uplinks
System OID String: 1.3.6.1.4.1.259.8.1.9
System information
 System Up time: 0 days, 1 hours, 23 minutes, and 44.61 seconds
 System Name             : [NONE]
 System Location         : [NONE]
 System Contact          : [NONE]
 MAC Address (Unit1):      00-20-1A-DF-9C-A0
 MAC Address (Unit2):      00-20-1A-DF-9E-C0
 Web Server:              Enabled
 Web Server Port:         80
 Web Secure Server:       Enabled
 Web Secure Server Port:  443
 Telnet Server:           Enable
 Telnet Server Port:      23
 Jumbo Frame:             Disabled
 Jumbo Frame Size:        1522

 POST Result:
DUMMY Test 1 ................. PASS
DRAM Test .................... PASS
PCI Device 1 Test ............ PASS
I2C Bus Initialization ....... PASS
Fan Speed Test ............... PASS

Done All Pass.
Console#
```

show users

Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a “*” symbol next to the Line (i.e., session) index number.

Example

```
Console#show users
 Username accounts:
  Username Privilege Public-Key
  -------- --------- ----------
     admin        15       None
     guest         0       None
     steve        15        RSA

 Online users:
  Line            Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ---------------- ---------------
  0   console     admin           0:14:14
* 1      VTY 0    admin           0:00:00     192.168.1.19
  2      SSH 1    steve           0:00:06     192.168.1.19

 Web online users:
  Line            Remote IP addr Username Idle time (h:m:s).
  ----------- ------------- -------- -----------------
 1      HTTP   192.168.1.19     admin            0:00:00

Console#
```

show version

This command displays hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See “Displaying Switch Hardware/Software Versions” on page 4-3 for detailed information on the items displayed by this command.

Example

```
Console#show version
Unit 1
 Serial Number:            0000E8900001
 Hardware Version:         R01
 EPLD Version:             1.06
 Number of Ports:          26
 Main Power Status:        Up
 Redundant Power Status:   Not present

Agent (Master)
 Unit ID:                  1
 Loader Version:           1.19.2.58
 Boot ROM Version:         1.1.0.1
 Operation Code Version:   1.1.0.2

Console#
```

Frame Size Commands

This section describes commands used to configure the Ethernet frame size on the switch.

Table 23-4 Frame Size Commands

Command	Function	Mode	Page
jumbo frame	Enables support for jumbo frames	GC	23-9

jumbo frame

This command enables support for jumbo frames. Use the **no** form to disable it.

Syntax

[**no**] **jumbo frame**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- This switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.
- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex

connections, all devices in the collision domain would need to support jumbo frames.

- The current setting for jumbo frames can be displayed with the **show system** command (page 23-7).

Example

```
Console(config)#jumbo frame
Console(config)#
```

Related Commands

show ipv6 mtu (41-19)

File Management Commands

Managing Firmware

Firmware can be uploaded and downloaded to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the switch to restore operation. The switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from a TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the switch.

Table 23-5 Flash/File Commands

Command	Function	Mode	Page
copy	Copies a code image or a switch configuration to or from flash memory or a TFTP server	PE	23-11
delete	Deletes a file or code image	PE	23-13
dir	Displays a list of files in flash memory	PE	23-14
whichboot	Displays the files booted	PE	23-15
boot system	Specifies the file or image used to start up the system	GC	23-16

copy

This command moves (upload/download) a code image or configuration file between the switch's flash memory and a TFTP server. When you save the system code or configuration settings to a file on a TFTP server, that file can later be downloaded to the switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

copy file {**file** | **running-config** | **startup-config** | **tftp** | **unit**}
copy running-config {**file** | **startup-config** | **tftp**}
copy startup-config {**file** | **running-config** | **tftp**}
copy tftp {**file** | **running-config** | **startup-config** | **https-certificate** | **public-key**}
copy unit file

- **file** - Keyword that allows you to copy to/from a file.
- **running-config** - Keyword that allows you to copy to/from the current running configuration.
- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that allows you to copy to/from a TFTP server.
- **https-certificate** - Keyword that allows you to copy the HTTPS secure site certificate.
- **public-key** - Keyword that allows you to copy a SSH key from a TFTP server. (See "Secure Shell Commands" on page 25-15.)
- **unit** - Keyword that allows you to copy to/from a specific unit in the stack.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- You can use "Factory_Default_Config.cfg" as the source to copy from the factory default configuration file, but you cannot use it as the destination.
- To replace the startup configuration, you must use **startup-config** as the destination.

- Use the **copy file** unit command to copy a local file to another switch in the stack. Use the **copy unit file** command to copy a file from another switch in the stack.
- The Boot ROM and Loader cannot be uploaded or downloaded from the TFTP server. You must follow the instructions in the release notes for new firmware, or contact your distributor for help.
- For information on specifying an https-certificate, see “Replacing the Default Secure-site Certificate” on page 6-7. For information on configuring the switch to use HTTPS for a secure connection, see “ip http secure-server” on page 25-12.

Example

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
 1. config:  2. opcode: <1-2>: 2
Source file name: V3.1.16.20.BIX
Destination file name: V311620
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
 1. config:  2. opcode: <1-2>: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name: startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: ********

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication via SSH is only supported for users configured locally on the switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
 1. RSA:  2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

delete

This command deletes a file or image.

Syntax

delete [*unit*:] *filename*

- *filename* - Name of configuration file or code image.
- *unit* - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.
- A colon (:) is required after the specified unit number.

Example

This example shows how to delete the test2.cfg configuration file from flash memory.

```
Console#delete test2.cfg
Console#
```

Related Commands

dir (23-14)
delete public-key (25-20)

dir

This command displays a list of files in flash memory.

Syntax

dir [*unit*:] {{**boot-rom:** | **config:** | **opcode:**} [*filename*]}

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file.
- **config** - Switch configuration file.
- **opcode** - Run-time operation code image file.
- *filename* - Name of configuration file or code image. If this file exists but contains errors, information on this file cannot be shown.
- *unit* - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If you enter the command **dir** without any parameters, the system displays all files.
- A colon (:) is required after the specified unit number.

- File information is shown below:

Table 23-6 File Directory Information

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

The following example shows how to display all file information:

```
Console#dir
          File name                        File type        Startup Size (byte)
 -----------------------------------        -------------   ------- -----------
 Unit1:
 Unit1:
          IC40240_480F_DIAG_V1.1.0.1.BIX      Boot-Rom Image   Y             1595976
          IC40240_480F-FLF_V1.1.0.2.BIX       Operation Code   Y              4973264
          Factory_Default_Config.cfg        Config File      N                  455
          startup1.cfg                      Config  File      Y                 3653
 ---------------------------------------------------------------------------
                                                   Total free space:    58851328
Console#
```

whichboot

This command displays which files were booted when the system powered up.

Syntax

whichboot [*unit*]

unit - Stack unit. (Range: 1-8)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```
Console#whichboot
                        File name        File type Startup Size (byte)
 -------------------------------- -------------- ------- -----------
 Unit1:
          IC40240_480F_DIAG_V1.1.0.1.BIX      Boot-Rom Image   Y             1595976
          IC40240_480F-FLF-38_V1.1.0.2.BIX    Operation Code   Y             4973264
          startup1.cfg                      Config  File      Y                3653
Console#
```

boot system

This command specifies the file or image used to start up the system.

Syntax

boot system [*unit*:] {**boot-rom**| **config** | **opcode**}: *filename*

The type of file or image to set as a default includes:

- **boot-rom*** - Boot ROM.
- **config*** - Configuration file.
- **opcode*** - Run-time operation code.
- *filename* - Name of configuration file or code image.
- *unit** - Stack unit. (Range: 1-8)

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified unit number and file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

dir (23-14)
whichboot (23-15)

Line Commands

You can access the onboard configuration program by attaching a VT100 compatible device to the server's serial port. These commands are used to set communication parameters for the serial port or Telnet (i.e., a virtual terminal).

Table 23-7 Line Commands

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	23-17
login	Enables password checking at login	LC	23-18
password	Specifies a password on a line	LC	23-19
timeout login response	Sets the interval that the system waits for a login attempt	LC	23-20
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	23-20
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	23-21
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command	LC	23-22
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	23-22
parity*	Defines the generation of a parity bit	LC	23-23
speed*	Sets the terminal baud rate	LC	23-23
stopbits*	Sets the number of the stop bits transmitted per byte	LC	23-24
disconnect	Terminates a line connection	PE	23-24
show line	Displays a terminal line's parameters	NE, PE	23-25

* These commands only apply to the serial port.

line

This command identifies a specific line for configuration, and to process subsequent line configuration commands.

Syntax

line {**console** | **vty**}

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as "VTY" in screen displays such as **show users**. However, the serial communication parameters (e.g., databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (23-25)
show users (23-8)

login

This command enables password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]
no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the switch itself at login:
  - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
  - **login local** selects authentication via the user name and password specified by the **username** command (i.e., default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
  - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication via the switch itself. To configure user names and passwords for remote authentication servers, you must use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (25-2)
password (23-19)

password

This command specifies the password for a line. Use the **no** form to remove the password.

Syntax

password {**0** | **7**} *password*
no password

- {**0** | **7**} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If you enter the correct password, the system shows a prompt. You can use the **password-thresh** command to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (23-18)
password-thresh (23-21)

timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

Syntax

timeout login response [*seconds*]
no timeout login response

seconds - Integer that specifies the timeout interval.
(Range: 0 - 300 seconds; 0: disabled)

Default Setting

- CLI: Disabled (0 seconds)
- Telnet: 300 seconds

Command Mode

Line Configuration

Command Usage

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

exec-timeout

This command sets the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout [*seconds*]
no exec-timeout

seconds - Integer that specifies the timeout interval.
(Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

CLI: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

password-thresh

This command sets the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh [*threshold*]
no password-thresh

threshold - The number of allowed password attempts.
(Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (23-22)

silent-time

This command sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time [*seconds*]
no silent-time

seconds - The number of seconds to disable console response. (Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration (console only)

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (23-21)

databits

This command sets the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {**7** | **8**}
no databits

- 7 - Seven data bits per character.
- 8 - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (23-23)

parity

This command defines the generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

parity {**none** | **even** | **odd**}
no parity

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none
Console(config-line)#
```

speed

This command sets the terminal line’s baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed *bps*
no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, 115200 bps, or auto)

Default Setting

auto

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the speed you selected is not supported. If you select the “auto” option, the switch will automatically detect the baud rate configured on the attached terminal, and adjust the speed accordingly.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

stopbits

This command sets the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {**1** | **2**}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

disconnect

This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect *session-id*

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier “0” will disconnect the console connection. Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

show ssh (25-22)
show users (23-8)

show line

This command displays the terminal line’s parameters.

Syntax

show line [**console** | **vty**]

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (i.e., Telnet).

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
 Console configuration:
  Password threshold:  3 times
  Interactive timeout: Disabled
  Login timeout: Disabled
  Silent time:         Disabled
  Baudrate:            auto
  Databits:            8
  Parity:              none
  Stopbits:            1

 VTY configuration:
  Password threshold:  3 times
  Interactive timeout: 600 sec
  Login timeout: 300 sec
Console#
```

Event Logging Commands

This section describes commands used to configure event logging on the switch.

Table 23-8 Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	23-26
logging history	Limits syslog messages saved to switch memory based on severity	GC	23-27
logging host	Adds a syslog server host IP address that will receive logging messages	GC	23-28
logging facility	Sets the facility type for remote logging of syslog messages	GC	23-28
logging trap	Limits syslog messages saved to a remote server based on severity	GC	23-29
clear log	Clears messages from the logging buffer	PE	23-29
show logging	Displays the state of logging	PE	23-30
show log	Displays log messages	PE	23-31

logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

[**no**] **logging on**

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. You can use the **logging history** command to control the type of error messages that are stored in memory. You can use the **logging trap** command to control the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (23-27)
logging trap (23-29)
clear log (23-29)

logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

logging history {**flash** | **ram**} *level*
no logging history {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).
- *level* - One of the levels listed below. Messages sent include the selected level down to level 0. (Range: 0-7)

Table 23-9 Logging Levels

Level	Severity Name	Description
7	debugging	Debugging messages
6	informational	Informational messages only
5	notifications	Normal but significant condition, such as cold start
4	warnings	Warning conditions (e.g., return false, unexpected return)
3	errors	Error conditions (e.g., invalid input, default used)
2	critical	Critical conditions (e.g., memory allocation, or free memory error - resource exhausted)
1	alerts	Immediate action needed
0	emergencies	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (i.e., numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0
Console(config)#
```

logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

[**no**] **logging host** *host_ip_address*

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use this command more than once to build up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3
Console(config)#
```

logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

[**no**] **logging facility** *type*

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

Syntax

logging trap [*level*]
no logging trap

level - One of the syslog severity levels listed in the table on page 23-27. Messages sent include the selected level up through level 0.

Default Setting

- Disabled
- Level 7 - 0

Command Mode

Global Configuration

Command Usage

- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

Example

```
Console(config)#logging trap 4
Console(config)#
```

clear log

This command clears messages from the log buffer.

Syntax

clear log [**flash** | **ram**]

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear log
Console#
```

Related Commands

show log (23-31)

show logging

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

show logging {**flash** | **ram** | **sendmail** | **trap**}

- **flash** - Displays settings for storing event messages in flash memory (i.e., permanent memory).
- **ram** - Displays settings for storing event messages in temporary RAM (i.e., memory flushed on power reset).
- **sendmail** - Displays settings for the SMTP event handler (page 23-35).
- **trap** - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is “errors” (i.e., default level 3 - 0), and the message level for RAM is “debugging” (i.e., default level 7 - 0).

```
Console#show logging flash
Syslog logging:             Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:             Enabled
History logging in RAM: level debugging
Console#
```

Table 23-10 show logging flash/ram - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
History logging in FLASH	The message level(s) reported based on the **logging history** command.
History logging in RAM	The message level(s) reported based on the **logging history** command.

The following example displays settings for the trap function.

```
Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type:           Debugging messages
REMOTELOG server IP address: 1.2.3.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#
```

Table 23-11 show logging trap - display description

Field	Description
Syslog logging	Shows if system logging has been enabled via the **logging on** command.
REMOTELOG status	Shows if remote logging has been enabled via the **logging trap** command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the **logging facility** command.
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the **logging trap** command.
REMOTELOG server IP address	The address of syslog servers as specified in the **logging host** command.

Related Commands

show logging sendmail (23-35)

show log

This command displays the log messages stored in local memory.

Syntax

show log {**flash** | **ram**}

- **flash** - Event history stored in flash memory (i.e., permanent memory).
- **ram** - Event history stored in temporary RAM (i.e., memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the event message stored in RAM.

```
Console#show log ram
[1] 00:01:30 2001-01-01
   "VLAN 1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
   "Unit 1, Port  1 link-up notification."
   level: 6, module: 5, function: 1, and event no.: 1
Console#
```

SMTP Alert Commands

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 23-12 SMTP Alert Commands

Command	Function	Mode	Page
logging sendmail host	SMTP servers to receive alert messages	GC	23-32
logging sendmail level	Severity threshold used to trigger alert messages	GC	23-33
logging sendmail source-email	Email address used for “From” field of alert messages	GC	23-33
logging sendmail destination-email	Email recipients of alert messages	GC	23-34
logging sendmail	Enables SMTP event handling	GC	23-34
show logging sendmail	Displays SMTP event handler settings	NE, PE	23-35

logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

[**no**] **logging sendmail host** *ip_address*

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- You can specify up to three SMTP servers for event handing. However, you must enter a separate command to specify each server.

- To send email alerts, the switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19
Console(config)#
```

logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

logging sendmail level *level*

level - One of the system message levels (page 23-27). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3
Console(config)#
```

logging sendmail source-email

This command sets the email address used for the “From” field in alert messages.

Syntax

logging sendmail source-email *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You may use an symbolic email address that identifies the switch, or the address of an administrator responsible for the switch.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com
Console(config)#
```

logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

[**no**] **logging sendmail destination-email** *email-address*

email-address - The source email address used in alert messages. (Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

You can specify up to five recipients for alert messages. However, you must enter a separate command to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-company.com
Console(config)#
```

logging sendmail

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

[**no**] **logging sendmail**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail
Console(config)#
```

show logging sendmail

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show logging sendmail
SMTP servers
-----------------------------------------------
192.168.1.19

SMTP minimum severity level: 7

SMTP destination email addresses
-----------------------------------------------
ted@this-company.com

SMTP source email address: bill@this-company.com

SMTP status: Enabled
Console#
```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the switch will only record the time from the factory default set at the last bootup.

Table 23-13 Time Commands

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	23-36
sntp server	Specifies one or more time servers	GC	23-37
sntp poll	Sets the interval at which the client polls for time	GC	23-37
sntp update-time	Sends a request to immediately update the time	GC	23-38
show sntp	Shows current SNTP configuration settings	NE, PE	23-38
clock timezone	Sets the time zone for the switch’s internal clock	GC	23-39
clock timezone-predefined	Sets the time zone for the switch’s internal clock using predefined time zone configurations	GC	23-39

Table 23-13 Time Commands (Continued)

Command	Function	Mode	Page
clock summertime (date)	Configures summer time (daylight savings time) for the switch’s internal clock	GC	23-40
clock summertime (predefined)	Configures summer time (daylight savings time) for the switch’s internal clock	GC	23-41
clock summertime (recurring)	Configures summer time (daylight savings time) for the switch’s internal clock	GC	23-42
show clock	Shows the time zone and summer-time settings	PE	23-43
calendar set	Sets the system date and time	PE	23-44
show calendar	Displays the current date and time setting	NE, PE	23-44

sntp client

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form to disable SNTP client requests.

Syntax

[**no**] **sntp client**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the switch only records the time starting from the factory default set at the last bootup (i.e., 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified via the **sntp servers** command. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console(config)#sntp poll 60
Console(config)#sntp client
Console(config)#end
Console#show sntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

Related Commands

sntp server (23-37)
sntp poll (23-37)
show sntp (23-38)

sntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use the this command with no arguments to clear all time servers from the current list.

Syntax

sntp server [*ip1* [*ip2* [*ip3*]]]

ip - IP address of an time server (NTP or SNTP). (Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set via the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (23-36)
sntp poll (23-37)
show sntp (23-38)

sntp poll

This command sets the interval between sending time requests when the switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll *seconds*
no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (23-36)

sntp update-time

This command sends a request to the configured SNTP servers to immediately update the time.

Command Mode

Global Configuration

Example

```
Console(config)#sntp update-time
Console(config)#
```

Related Commands

sntp client (23-36)
sntp server (23-37)

show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (i.e., unicast).

Example

```
Console#show sntp
Current time:  Dec 23 05:13:28 2002
Poll interval: 16
Current mode:    unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

clock timezone

This command sets the time zone for the switch's internal clock.

Syntax

clock timezone *name* **hour** *hours* **minute** *minutes* {**before-utc** | **after-utc**}

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before/after UTC. (Range: 0-13 hours)
- *minutes* - Number of minutes before/after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (23-38)

clock timezone-predefined

This command uses predefined time zone configurations to set the time zone for the switch's internal clock. Use the **no** form to restore the default.

Syntax

clock timezone-predefined *offset-city*
no clock timezone-predefined

- *offset* - Select the offset from GMT. (Range: GMT-0100 - GMT-1200; GMT-Greenwich-Mean-Time; GMT+0100 - GMT+1400)
- *city* - Select the city associated with the chosen GMT offset. After the offset has been entered, use the tab-complete function to display the available city options.

Default Setting

GMT-Greenwich-Mean-Time-Dublin,Edinburgh,Lisbon,London

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to your local time, you must indicate the number of hours and minutes your time zone is east (before) or west (after) of UTC.

Example

```
Console(config)#clock timezone-predefined GMT-0930-Taiohae
Console(config)#
```

Related Commands

show clock (23-43)

clock summer-time (date)

This command sets the start, end, and offset times of summer-time (daylight savings time) for the switch on a one-time basis. Use the **no** form to disable summer-time.

Syntax

clock summer-time *name* **date** *b-month b-day b-year b-hour b-minute*
e-month e-day e-year e-hour e-minute offset
no clock summer-time

- *name* - Name of the time zone while summer-time is in effect, usually an acronym. (Range: 1-30 characters)
- *b-month* - The month when summer-time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)
- *b-day* - The day summer-time will begin. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)
- *b-year*- The year summer-time will begin.
- *b-hour* - The hour summer-time will begin. (Range: 0-23 hours)
- *b-minute* - The minute summer-time will begin. (Range: 0-59 minutes)
- *e-month* - The month when summer-time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)
- *e-day* - The day summer-time will end. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)
- *e-year*- The year summer-time will end.
- *e-hour* - The hour summer-time will end. (Range: 0-23 hours)
- *e-minute* - The minute summer-time will end. (Range: 0-59 minutes)

- *offset* - Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- This command sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer-time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

Example

```
Console(config)#clock summer-time DEST date april 1 2007 23 23 april 23
  2007 23 23 60
Console(config)#
```

Related Commands

show clock (23-43)

clock summer-time (predefined)

This command configures the summer time (daylight savings time) status and settings for the switch using predefined configurations for several major regions of the world. Use the **no** form to disable summer time.

Syntax

clock summer-time *name* **predefined** [**australia** | **europe** | **new-zealand** | **usa**]

no clock summer-time

name - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- This command sets the summer-time time relative to the configured time zone. To specify the time corresponding to your local time when summer-time is in effect, select the predefined summer-time time zone appropriate for your location, or manually configure summer-time if these predefined configurations do not apply to your location (see **clock summer-time** (date) on page 23-40 or **clock summer-time** (recurring) on page 23-42).

Table 23-14 Predefined Summer-Time Parameters

Region	Start Time, Day, Week, & Month	End Time, Day, Week, & Month	Rel. Offset
Australia	00:00:00, Sunday, Week 5 of October	23:59:59, Sunday, Week 5 of March	60 min
Europe	00:00:00, Sunday, Week 5 of March	23:59:59, Sunday, Week 5 of October	60 min
New Zealand	00:00:00, Sunday, Week 1 of October	23:59:59, Sunday, Week 3 of March	60 min
USA	02:00:00, Sunday, Week 2 of March	02:00:00, Sunday, Week 1 of November	60 min

Example

```
Console(config)#clock summer-time MESZ predefined europe
Console(config)#
```

Related Commands

show clock (23-43)

clock summer-time (recurring)

This command allows the user to manually configure the start, end, and offset times of summer-time (daylight savings time) for the switch on a recurring basis. Use the **no** form to disable summer-time.

Syntax

clock summer-time *name* **recurring** *b-week b-day b-month b-hour b-minute e-week e-day e-month e-hour e-minute offset*
no clock summer-time

- *name* - Name of the timezone while summer time is in effect, usually an acronym. (Range: 1-30 characters)
- *b-week* - The week of the month when summer-time will begin. (Range: 1-5)
- *b-day* - The day of the week when summer-time will begin. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)

- *b-month* - The month when summer-time will begin. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)
- *b-hour* - The hour when summer-time will begin. (Range: 0-23 hours)
- *b-minute* - The minute when summer-time will begin. (Range: 0-59 minutes)
- *e-week* - The week of the month when summer-time will end. (Range: 1-5)
- e-day - The day of the week summer-time will end. (Options: **sunday** | **monday** | **tuesday** | **wednesday** | **thursday** | **friday** | **saturday**)
- *e-month* - The month when summer-time will end. (Options: **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**)
- *e-hour* - The hour when summer-time will end. (Range: 0-23 hours)
- *e-minute* - The minute when summer-time will end. (Range: 0-59 minutes)
- *offset* - Summer-time offset from the regular time zone, in minutes. (Range: 0-99 minutes)

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- In some countries or regions, clocks are adjusted through the summer months so that afternoons have more daylight and mornings have less. This is known as Summer Time, or Daylight Savings Time (DST). Typically, clocks are adjusted forward one hour at the start of spring and then adjusted backward in autumn.
- This command sets the summer-time time zone relative to the currently configured time zone. To specify a time corresponding to your local time when summer-time is in effect, you must indicate the number of minutes your summer-time time zone deviates from your regular time zone.

Example

```
Console(config)#clock summer-time MESZ recurring 1 friday june 23 59 3
  saturday september 2 55 60
Console(config)#
```

Related Commands

show clock (23-43)

show clock

This command shows the time zone and summer-time settings.

Command Mode

Privileged Exec

Example

```
Console#show clock
 Time Zone               : GMT-0930-Taiohaer
 Summer Time             : offset 60 minutes
                          Apr 1 2007 23:23 to Apr 23 2007 23:23
 Summer Time in Effect : No
Console#
```

calendar set

This command sets the system clock. It may be used if there is no time server on your network, or if you have not configured the switch to receive signals from a time server.

Syntax

calendar set *hour min sec* {*day month year* | *month day year*}

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *min* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **january** | **february** | **march** | **april** | **may** | **june** | **july** | **august** | **september** | **october** | **november** | **december**
- *year* - Year (4-digit). (Range: 2001 - 2100)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, February 1st, 2002.

```
Console#calendar set 15 12 34 february 1 2002
Console#
```

show calendar

This command displays the system clock.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show calendar
 15:12:34 February 1 2002
Console#
```

Chapter 24: SNMP Commands

Controls access to this switch from management stations using the Simple Network Management Protocol (SNMP), as well as the error types sent to trap managers.

SNMP Version 3 also provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use SNMPv3, first set an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (i.e., SNMP v1, v2c or v3) and security level (i.e., authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 24-1 SNMP Commands

Command	Function	Mode	Page
snmp-server	Enables the SNMP agent	GC	24-2
show snmp	Displays the status of SNMP communications	NE, PE	24-2
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	24-3
snmp-server contact	Sets the system contact string	GC	24-4
snmp-server location	Sets the system location string	GC	24-4
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	24-5
snmp-server enable traps	Enables the device to send SNMP traps (i.e., SNMP notifications)	GC	24-7
snmp-server engine-id	Sets the SNMP engine ID	GC	24-8
show snmp engine-id	Shows the SNMP engine ID	PE	24-9
snmp-server view	Adds an SNMP view	GC	24-10
show snmp view	Shows the SNMP views	PE	24-11
snmp-server group	Adds an SNMP group, mapping users to views	GC	24-11
show snmp group	Shows the SNMP groups	PE	24-12
snmp-server user	Adds a user to an SNMP group	GC	24-14
show snmp user	Shows the SNMP users	PE	24-15

snmp-server

This command enables the SNMPv3 engine and services for all management clients (i.e., versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[**no**] **snmp-server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

show snmp

This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP Agent: enabled

SNMP traps:
 Authentication: enable
   Link-up-down: enable

SNMP communities:
   1. private, and the privilege is read-write
   2. public, and the privilege is read-only

0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Set-request PDUs
0 SNMP packets output
    0 Too big errors
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs

SNMP logging: disabled
Console#
```

snmp-server community

This command defines the SNMP v1 and v2c community access string. Use the **no** form to remove the specified community string.

Syntax

snmp-server community *string* [**ro**|**rw**]
no snmp-server community *string*

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- public - Read-only access. Authorized management stations are only able to retrieve MIB objects.

- private - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw
Console(config)#
```

snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

snmp-server contact *string*
no snmp-server contact

string - String that describes the system contact information. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul
Console(config)#
```

Related Commands

snmp-server location (24-4)

snmp-server location

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

snmp-server location *text*
no snmp-server location

text - String that describes the system location. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location WC-19
Console(config)#
```

Related Commands

snmp-server contact (24-4)

snmp-server host

This command specifies the recipient of a Simple Network Management Protocol notification operation. Use the **no** form to remove the specified host.

Syntax

snmp-server host *host-addr* [**inform** [**retry** *retries* | **timeout** *seconds*]] *community-string* [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} [**udp-port** *port*]}

no snmp-server host *host-addr*

- *host-addr* - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- **inform** - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
  - *retries* - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
  - *seconds* - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- *community-string* - Password-like community string sent with the notification operation to SNMP V1 and V2c hosts. Although you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP Version 1, 2c or 3 traps. (Range: 1, 2c, 3; Default: 1)
  - **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” on page 5-1 for further information about these authentication and encryption options.
- *port* - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

- Host Address: None
- Notification Type: Traps

- SNMP Version: 1
- UDP Port: 162

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. In order to enable multiple hosts, you must issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- Notifications are issued by the switch as trap messages by default. The recipient of a trap message does not send a response to the switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. You should consider these effects when deciding whether to issue notifications as traps or informs.

  To send an inform to a SNMPv2c host, complete these steps:

  1. Enable the SNMP agent (page 24-2).
  2. Allow the switch to send SNMP traps; i.e., notifications (page 24-7).
  3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
  4. Create a view with the required notification messages (page 24-10).
  5. Create a group that includes the required notify view (page 24-11).

  To send an inform to a SNMPv3 host, complete these steps:

  1. Enable the SNMP agent (page 24-2).
  2. Allow the switch to send SNMP traps; i.e., notifications (page 24-7).
  3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
  4. Create a view with the required notification messages (page 24-10).
  5. Create a group that includes the required notify view (page 24-11).
  6. Specify a remote engine ID where the user resides (page 24-8).
  7. Then configure a remote user (page 24-14).

- The switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.

- If you specify an SNMP Version 3 host, then the community string is interpreted as an SNMP user name. If you use the V3 “auth” or “priv” options, the user name must first be defined with the **snmp-server user** command. Otherwise, the authentication password and/or privacy password will not exist, and the switch will not authorize SNMP access for the host. However, if you specify a V3 host with the “noauth” option, an SNMP user account will be generated, and the switch will authorize SNMP access for the host.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (24-7)

snmp-server enable traps

This command enables this device to send Simple Network Management Protocol traps or informs (i.e., SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

[**no**] **snmp-server enable traps** [**authentication** | **link-up-down**]

- **authentication** - Keyword to issue authentication failure notifications.
- **link-up-down** - Keyword to issue link-up or link-down notifications.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure this device to send SNMP notifications, you must enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, both authentication and link-up-down notifications are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled.
- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in

conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command (page 24-11).

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (24-5)

snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

snmp-server engine-id {**local** | **remote** {*ip-address*}} *engineid-string*
no snmp-server engine-id {**local** | **remote** {*ip-address*}}

- **local** - Specifies the SNMP engine on this switch.
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- *engineid-string* - String identifying the engine ID. (Range: 9-64 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- An SNMP engine is an independent SNMP agent that resides either on this switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See **snmp-server host** on page 24-5.) The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore need to configure the remote agent's SNMP engine ID before you can send proxy requests or informs to it.
- If an odd number of characters are specified, a trailing zero is added to the value to fill in the missing octet. For example, the value "123456789" is equivalent to "1234567890".

- A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. You will need to reconfigure all existing users (page 24-14).

Example

```
Console(config)#snmp-server engine-id local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#
```

Related Commands

snmp-server host (24-5)

show snmp engine-id

This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                                         IP address
80000000030004e2b316c54321                                   192.168.1.19
Console#
```

Table 24-2 show snmp engine-id - display description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

snmp-server view

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

snmp-server view *view-name oid-tree* {**included** | **excluded**}
no snmp-server view *view-name*

- *view-name* - Name of an SNMP view. (Range: 1-32 characters)
- *oid-tree* - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)
- **included** - Defines an included view.
- **excluded** - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- Views are used in the **snmp-server group** command to restrict user access to specified portions of the MIB tree.
- The predefined view “defaultview” includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wild card is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2 included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.* included
Console(config)#
```

show snmp view

This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```
Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

Console#
```

Table 24-3 show snmp view - display description

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

snmp-server group *groupname* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}
[**read** *readview*] [**write** *writeview*] [**notify** *notifyview*]
no snmp-server group *groupname*

- *groupname* - Name of an SNMP group. (Range: 1-32 characters)
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **auth** | **noauth** | **priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” on page 5-1 for further information about these authentication and encryption options.
- *readview* - Defines the view for read access. (1-32 characters)
- *writeview* - Defines the view for write access. (1-32 characters)
- *notifyview* - Defines the view for notifications. (1-32 characters)

Default Setting

- Default groups: public[24] (read only), private[25] (read/write)
- *readview* - Every object belonging to the Internet OID space (1.3.6.1).
- writeview - Nothing is defined.
- *notifyview* - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- A group sets the access policy for the assigned users.
- When authentication is selected, the MD5 or SHA algorithm is used as specified in the **snmp-server user** command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- For additional information on the notification messages supported by this switch, see “Supported Notification Messages” on page 5-14. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the **snmp-server enable traps** command (page 24-7).

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active
```

[24] No view is defined.

[25] Maps to the defaultview.

```
Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#
```

Table 24-4 show snmp group - display description

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

Syntax

snmp-server user *username groupname* [**remote** *ip-address*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password* [**priv des56** *priv-password*]]
no snmp-server user *username* {**v1** | **v2c** | **v3** | **remote**}

- *username* - Name of user connecting to the SNMP agent. (Range: 1-32 characters)
- *groupname* - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- **v1** | **v2c** | **v3** - Use SNMP version 1, 2c or 3.
- **encrypted** - Accepts the password as encrypted input.
- **auth** - Uses SNMPv3 with authentication.
- **md5** | **sha** - Uses MD5 or SHA authentication.
- *auth-password* - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)
- **priv des56** - Uses SNMPv3 with privacy with DES56 encryption.
- *priv-password* - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. You should therefore configure the engine ID with the **snmp-server engine-id** command before using this configuration command.
- Before you configure a remote user, use the **snmp-server engine-id** command (page 24-8) to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. You therefore

need to configure the remote agent’s SNMP engine ID before you can send proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve group r&d v3 auth md5 greenpeace
 priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19 v3
 auth md5 greenpeace priv des56 einstien
Console(config)#
```

show snmp user

This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

```
Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#
```

Table 24-5 show snmp user - display description

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authentication Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

Chapter 25: User Authentication Commands

You can configure this switch to authenticate users logging into the system for management access using local or remote authentication methods. You can also enable port-based authentication for network client access using IEEE 802.1X.

Table 25-1 Authentication Commands

Command Group	Function	Page
User Accounts	Configures the basic user names and passwords for management access	25-1
Authentication Sequence	Defines logon authentication method and precedence	25-4
RADIUS Client	Configures settings for authentication via a RADIUS server	25-6
TACACS+ Client	Configures settings for authentication via a TACACS+ server	25-9
Web Server Settings	Enables management access via a web browser	25-11
Telnet Server Settings	Enables management access via Telnet	25-14
Secure Shell Settings	Provides secure replacement for Telnet	25-15
Port Security	Configures secure addresses for a port	25-24
Port Authentication	Configures host authentication on specific ports using 802.1X	25-26
Management IP Filter	Configures IP addresses that are allowed management access	25-35

User Account Commands

The basic commands required for management access are listed in this section. This switch also includes other options for password checking via the console or a Telnet connection (page 23-17), user authentication via a remote authentication server (page 25-1), and host access authentication for specific ports (page 25-26).

Table 25-2 User Access Commands

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	25-2
enable password	Sets a password to control access to the Privileged Exec level	GC	25-3

username

This command adds named users, requires authentication at login, specifies or changes a user's password (or specify that no password is required), or specifies or changes a user's access level. Use the **no** form to remove a user name.

Syntax

username *name* {**access-level** *level* | **nopassword** |
  password {**0** | **7**} *password*}
no username *name*

- *name* - The name of the user.
  (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level** *level* - Specifies the user level.
  The device has two predefined privilege levels:
  0: Normal Exec, **15**: Privileged Exec.
- **nopassword** - No password is required for this user to log in.
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- **password** *password* - The authentication password for the user.
  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default access level is Normal Exec.
- The factory defaults for the user names and passwords are:

Table 25-3 Default Login Settings

username	access-level	password
guest admin	0 15	guest admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

This example shows how the set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

enable password

After initially logging onto the system, you should set the Privileged Exec password. Remember to record it in a safe place. This command controls access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

enable password [**level** *level*] {**0** | **7**} *password*
no enable password [**level** *level*]

- **level** *level* - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {**0** | **7**} - 0 means plain password, 7 means encrypted password.
- *password* - password for this privilege level.
  (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- The default password is “super”

Command Mode

Global Configuration

Command Usage

- You cannot set a null password. You will have to enter a password to change the command mode from Normal Exec to Privileged Exec with the **enable** command (page 22-1).
- The encrypted password is required for compatibility with legacy password settings (i.e., plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need for you to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (22-1)
authentication enable (25-5)

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 25-4 Authentication Sequence Commands

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	25-4
authentication enable	Defines the authentication method and precedence for command mode change	GC	25-5

authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

authentication login {[**local**] [**radius**] [**tacacs**]}
no authentication login

- **local** - Use local password.
- **radius** - Use RADIUS server password.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter "**authentication login radius tacacs local**," the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username - for setting the local user names and passwords (25-2)

authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command (see page 22-1). Use the **no** form to restore the default.

Syntax

authentication enable {[**local**] [**radius**] [**tacacs**]}
no authentication enable

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- You can specify three authentication methods in a single command to indicate the authentication sequence. For example, if you enter “**authentication enable radius tacacs local**,” the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication enable radius
Console(config)#
```

Related Commands

enable password - sets the password for changing command modes (25-3)

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 25-5 RADIUS Client Commands

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	25-6
radius-server port	Sets the RADIUS server network port	GC	25-7
radius-server key	Sets the RADIUS encryption key	GC	25-7
radius-server retransmit	Sets the number of retries	GC	25-8
radius-server timeout	Sets the interval between sending authentication requests	GC	25-8
show radius-server	Shows the current RADIUS settings	PE	25-8

radius-server host

This command specifies primary and backup RADIUS servers and authentication parameters that apply to each server. Use the **no** form to restore the default values.

Syntax

[**no**] **radius-server** *index* **host** *host_ip_address* [**auth-port** *auth_port*] [**key** *key*] [**retransmit** *retransmit*] [**timeout** *timeout*]

- *index* - Allows you to specify up to five servers. These servers are queried in sequence until a server responds or the retransmit period expires.
- *host_ip_address* - IP address of server.
- *auth_port* - RADIUS server UDP port used for authentication messages. (Range: 1-65535)
- *key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)
- *retransmit* - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)
- *timeout* - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

- **auth-port** - 1812
- **timeout** - 5 seconds
- **retransmit** - 2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout 10
 retransmit 5 key green
Console(config)#
```

radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

radius-server port *port_number*
no radius-server port

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181
Console(config)#
```

radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

radius-server key *key_string*
no radius-server key

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

radius-server retransmit *number_of_retries*
no radius-server retransmit

number_of_retries - Number of times the switch will try to authenticate logon access via the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

radius-server timeout

This command sets the interval between transmitting authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

radius-server timeout *number_of_seconds*
no radius-server timeout

number_of_seconds - Number of seconds the switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

show radius-server

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS server configuration:

Global settings:
 Communication key with RADIUS server: *****
 Server port number:                   1812
 Retransmit times:                     2
 Request timeout:                      5

Server 1:
 Server IP address:                     192.168.1.1
 Communication key with RADIUS server: *****
 Server port number: 1812
 Retransmit times: 2
 Request timeout: 5

Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to a switch.

Table 25-6 TACACS+ Client Commands

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	25-9
tacacs-server port	Specifies the TACACS+ server network port	GC	25-10
tacacs-server key	Sets the TACACS+ encryption key	GC	25-10
show tacacs-server	Shows the current TACACS+ settings	GC	25-11

tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

tacacs-server host *host_ip_address*
no tacacs-server host

host_ip_address - IP address of a TACACS+ server.

Default Setting

10.11.12.13

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25
Console(config)#
```

tacacs-server port

This command specifies the TACACS+ server network port. Use the **no** form to restore the default.

Syntax

tacacs-server port *port_number*
no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181
Console(config)#
```

tacacs-server key

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

tacacs-server key *key_string*
no tacacs-server key

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 48 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green
Console(config)#
```

show tacacs-server

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show tacacs-server
Remote TACACS server configuration:
 Server IP address:                      10.11.12.13
 Communication key with TACACS server: *****
 Server port number:                     49
Console#
```

Web Server Commands

This section describes commands used to configure web browser management access to the switch.

Table 25-7   Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the web browser interface	GC	25-11
ip http server	Allows the switch to be monitored or configured from a browser	GC	25-12
ip http secure-server	Enables HTTPS (HTTP/SSL) for encrypted communications	GC	25-12
ip http secure-port	Specifies the UDP port number for HTTPS	GC	25-13

ip http port

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

ip http port *port-number*
no ip http port

port-number - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769
Console(config)#
```

Related Commands

ip http server (25-12)

ip http server

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

[**no**] **ip http server**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (25-11)

ip http secure-server

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (i.e., an encrypted connection) to the switch's web interface. Use the **no** form to disable this function.

Syntax

[**no**] **ip http secure-server**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the switch. However, you cannot configure the HTTP and HTTPS servers to use the same UDP port.
- If you enable HTTPS, you must indicate this in the URL that you specify in your browser: **https**://*device*[:*port_number*]

- When you start HTTPS, the connection is established in this way:
  - The client authenticates the server using the server's digital certificate.
  - The client and server negotiate a set of security protocols to use for the connection.
  - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

  A padlock icon should appear in the status bar for Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0.0.0 or above.
- The following web browsers and operating systems currently support HTTPS:

Table 25-8 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape 6.2 or later	Windows 98,Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6
Mozilla Firefox 2.0.0.0 or later	Windows 2000, Windows XP, Linux

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 6-7. Also refer to the **copy** command on page 23-11.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (25-13)
copy tftp https-certificate (23-11)

ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *port_number*

no ip http secure-port

port_number – The UDP port used for HTTPS. (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- You cannot configure the HTTP and HTTPS servers to use the same port.

- If you change the HTTPS port number, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://***device***:***port_number*

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (25-12)

Telnet Server Commands

This section describes commands used to configure Telnet management access to the switch.

Table 25-9 Telnet Server Commands

Command	Function	Mode	Page
ip telnet server	Allows the switch to be monitored or configured from Telnet; also specifies the port to be used by the Telnet interface	GC	25-11

ip telnet server

This command allows this device to be monitored or configured from Telnet. It also specifies the TCP port number used by the Telnet interface. Use the **no** form without the “port” keyword to disable this function. Use the **no** from with the “port” keyword to use the default port.

Syntax

ip telnet server [**port** *port-number*]
no telnet server [**port**]

- **port** - The TCP port used by the Telnet interface.
- *port-number* - The TCP port number to be used by the browser interface. (Range: 1-65535)

Default Setting

- Server: Enabled
- Server Port: 23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#ip telnet port 123
Console(config)#
```

Secure Shell Commands

This section describes the commands used to configure the SSH server. Note that you also need to install a SSH client on the management station when using this protocol to configure the switch.

Note: The switch supports both SSH Version 1.5 and 2.0 clients.

Table 25-10 Secure Shell Commands

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the switch	GC	25-17
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	25-18
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	25-19
ip ssh server-key size	Sets the SSH server key size	GC	25-19
copy tftp public-key	Copies the user’s public key from a TFTP server to the switch	PE	23-11
delete public-key	Deletes the public key for the specified user	PE	25-20
ip ssh crypto host-key generate	Generates the host key	PE	25-20
ip ssh crypto zeroize	Clear the host key from RAM	PE	25-21
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	25-21
disconnect	Terminates a line connection	PE	23-24
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	25-22
show ssh	Displays the status of current SSH sessions	PE	25-22
show public-key	Shows the public key for the specified user or for the host	PE	25-23
show users	Shows SSH users, including privilege level and public key type	PE	23-8

Configuration Guidelines

The SSH server on this switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or via a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 25-4. If public key authentication is specified by the client, then you must configure authentication keys on both the client and the switch as described in the following section. Note that regardless of whether you use public key or password authentication, you still have to generate authentication keys on the switch and enable the SSH server.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.

2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the switch. Otherwise, you need to manually create a known hosts file on the management station and place the host public key in it. An entry for a public key in the known hosts file would appear similar to the following example:

   ```
   10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
   15020245593199868544358361651999923329781766065830956 10825913212890233
   76546801726272571413428762941301196195566782 595664104869574278881462065
   1941746772984865468615717739390164779355942303577413098022737087794545
   24083971752646358058176716709574804776117
   ```

3. Import Client's Public Key to the Switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the switch. (Note that these clients must be configured locally on the switch with the **username** command as described on page 25-2.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA key:

   ```
   1024 35 134108168560989392104094492015542534763164192187295892114317388
   005553616163105177594083868631109291232226828519254374603100937187721199
   696317813662774141689851320491172048303392543241016379975923714490119380
   060902539484084827178194372288402533115952134861022902978982721353267131
   6294325328189150453063939166 43 steve@192.168.1.19
   ```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.

5. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the switch.

6. *Authentication* – One of the following authentication methods is employed:

   Password Authentication (for SSH v1.5 or V2 Clients)

   a. The client sends its password to the server.
   b. The switch compares the client's password to those stored in memory.
   c. If a match is found, the connection is allowed.

   Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, you do not need to configure the client's keys.

   Public Key Authentication – When an SSH client attempts to contact the switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the switch can access it. The following exchanges take place during this process:

Authenticating SSH v1.5 Clients

a. The client sends its RSA public key to the switch.

b. The switch compares the client's public key to those stored in memory.

c. If a match is found, the switch uses its secret key to generate a random 256-bit string as a challenge, encrypts this string with the user's public key, and sends it to the client.

d. The client uses its private key to decrypt the challenge string, computes the MD5 checksum, and sends the checksum back to the switch.

e. The switch compares the checksum sent from the client against that computed for the original string it sent. If the two checksums match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Authenticating SSH v2 Clients

a. The client first queries the switch to determine if DSA public key authentication using a preferred algorithm is acceptable.

b. If the specified algorithm is supported by the switch, it notifies the client to proceed with the authentication process. Otherwise, it rejects the request.

c. The client sends a signature generated using the private key to the switch.

d. When the server receives this message, it checks whether the supplied key is acceptable for authentication, and if so, it then checks whether the signature is correct. If both checks succeed, the client is authenticated.

Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

ip ssh server

This command enables the Secure Shell (SSH) server on this switch. Use the **no** form to disable this service.

Syntax

[**no**] **ip ssh server**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- You must generate DSA and RSA host keys before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (25-20)
show ssh (25-22)

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout *seconds*
no ip ssh timeout

seconds – The timeout for client response during SSH negotiation. (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (23-20)
show ip ssh (25-22)

ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

ip ssh authentication-retries *count*
no ip ssh authentication-retries

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (25-22)

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size *key-size*
no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

- The server key is a private key that is never shared outside the switch.
- The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

delete public-key

This command deletes the specified user’s public key.

Syntax

delete public-key *username* [**dsa** | **rsa**]

- *username* – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```

ip ssh crypto host-key generate

This command generates the host key pair (i.e., public and private).

Syntax

ip ssh crypto host-key generate [**dsa** | **rsa**]

- **dsa** – DSA (Version 2) key type.
- **rsa** – RSA (Version 1) key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- The switch uses only RSA Version 1 for SSHv1.5 clients and DSA Version 2 for SSHv2 clients.
- This command stores the host key pair in memory (i.e., RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, you must manually create a known hosts file and place the host public key in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#
```

Related Commands

ip ssh crypto zeroize (25-21)
ip ssh save host-key (25-21)

ip ssh crypto zeroize

This command clears the host key from memory (i.e. RAM).

Syntax

ip ssh crypto zeroize [**dsa** | **rsa**]

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH server must be disabled before you can execute this command.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (25-20)
ip ssh save host-key (25-21)
no ip ssh server (25-17)

ip ssh save host-key

This command saves the host key from RAM to flash memory.

Syntax

ip ssh save host-key

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (25-20)

show ip ssh

This command displays the connection settings used when authenticating client access to the SSH server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

show ssh

This command displays the current SSH server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State                Username Encryption
  0           2.0    Session-Started      admin       ctos aes128-cbc-hmac-md5
                                                 stoc aes128-cbc-hmac-md5
Console#
```

Table 25-11 show ssh - display description

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.

Table 25-11 show ssh - display description (Continued)

Field	Description
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5 *Terminology:* DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

show public-key

This command shows the public key for the specified user or for the host.

Syntax

show public-key [**user** [*username*]| **host**]

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.
- When an RSA key is displayed, the first field indicates the size of the host key (e.g., 1024), the second field is the encoded public exponent (e.g., 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```
Console#show public-key host
Host:
RSA:
1024 65537 13236940658254764031382795526536375927835525327972629521130241
0719421061655759424590939236096954050362775257556251003866130989393834523
1033280214988866192159556859887989191950588394018138744046890877916030583
7768185490002831341625008348718449522087429212255691665655296328163516964
0408315547660664151657116381
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2Hxc
YV44sXZ2JXhamLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKxl5fwFfv
JlPdOkFgzLGMinvSNYQwiQXbKTBH0Z4mUZpE85PWxDZMaCNBPjBrRAAAAFQChb4vsdfQGNIjw
bvwrNLaQ77isiwAAAIEAsy5YWDC99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR
2G395NLy5Qd7ZDxfA9mCOfT/yyEfbobMJZi8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm
iFq7O+jAhf1Dg45loAc27s6TLdtny1wRq/ow2eTCD5nekAAACBAJ8rMccXTxHLFAczWS7EjOy
DbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAwecsigF/+DjKGWtPNIQqabKgYCw2
o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwuHpOSKdxT3kk475S7
w0W
Console#
```

Port Security Commands

These commands can be used to enable port security on a port. When using port security, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take action by disabling the port and sending a trap message.

Table 25-12 Port Security Commands

Command	Function	Mode	Page
port security	Configures a secure port	IC	25-25
mac-address-table static	Maps a static address to a port in a VLAN	GC	31-1
show mac-address-table	Displays entries in the bridge-forwarding database	PE	31-3

port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

port security [**action** {**shutdown** | **trap** | **trap-and-shutdown**}
 | **max-mac-count** *address-count*]

no port security [**action** | **max-mac-count**]

- **action** - Response to take when port security is violated.
  - **shutdown** - Disable port only.
  - **trap** - Issue SNMP trap message only.
  - **trap-and-shutdown** - Issue SNMP trap message and disable port.
- **max-mac-count**
  - *address-count* - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

- Status: Disabled
- Action: None
- Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When port security is enabled with this command, the switch first clears all dynamically learned entries from the address table. It then starts learning new MAC addresses on the specified port, and stops learning addresses when it reaches a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port. (The specified maximum address count is effective when port security is enabled or disabled.)
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- You can also manually add secure addresses with the **mac-address-table static** command.
- A secure port has the following restrictions:
  - Cannot be connected to a network interconnection device.
  - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap
```

Related Commands

shutdown (27-7)
mac-address-table static (31-1)

802.1X Port Authentication

The switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 25-13 802.1X Port Authentication Commands

Command	Function	Mode	Page
dot1x system-auth-control	Enables dot1x globally on the switch.	GC	25-27
dot1x default	Resets all dot1x parameters to their default values	GC	25-27
dot1x max-req	Sets the maximum number of times that the switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC	25-27
dot1x port-control	Sets dot1x mode for a port interface	IC	25-28
dot1x operation-mode	Allows single or multiple hosts on an dot1x port	IC	25-29
dot1x re-authenticate	Forces re-authentication on specific ports	PE	25-30
dot1x re-authentication	Enables re-authentication for all ports	IC	25-30
dot1x timeout quiet-period	Sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC	25-31
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC	25-31
dot1x timeout tx-period	Sets the time period during an authentication session that the switch waits before re-transmitting an EAP packet	IC	25-32
show dot1x	Shows a l dot1x related information	PE	25-32

dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the switch. Use the **no** form to restore the default.

Syntax

[**no**] **dot1x system-auth-control**

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control
Console(config)#
```

dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default
Console(config)#
```

dot1x max-req

This command sets the maximum number of times the switch port will retransmit an EAP request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

dot1x max-req *count*
no dot1x max-req

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}
no dot1x port-control

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Command Usage

- 802.1X port authentication and port security cannot be configured together on the same port. Only one of these security mechanisms can be applied.
- 802.1X port authentication cannot be configured on trunk ports. In other words, a static trunk or dynamically configured trunk cannot be set to auto or force-unauthorized mode.
- When 802.1X authentication is enabled on a port, the MAC address learning function for this interface is disabled, and the addresses dynamically learned on this port are removed.
- Authenticated MAC addresses are stored as dynamic entries in the switch’s secure MAC address table. Configured static MAC addresses are added to the secure address table when seen on a switch port. Static addresses are treated as authenticated without sending a request to a RADIUS server.
- When port status changes to down, all MAC addresses are cleared from the secure MAC address table. Static VLAN assignments are not restored.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

dot1x operation-mode {**single-host** | **multi-host** [**max-count** *count*] | **mac-based-auth**}

no dot1x operation-mode [**multi-host max-count**]

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple hosts to connect to this port, with only one host needing to be authenticated.
- **max-count** – Keyword for the maximum number of hosts.

  count – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)
- **mac-based-auth** – Allows multiple hosts to connect to this port, with each host needing to be authenticated.

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- The “max-count” parameter specified by this command is only effective if the dot1x mode is set to “auto” by the dot1x port-control command (page 4-105).
- In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.
- In “mac-based-auth” mode, each host connected to a port needs to pass authentication. The number of hosts allowed access to a port operating in this mode is limited only by the available space in the secure address table (i.e., up to 1024 addresses).

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)

Command Mode

Privileged Exec

Command Usage

The re-authentication process verifies the connected client’s user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.

Example

```
Console#dot1x re-authenticate
Console#
```

dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

[**no**] **dot1x re-authentication**

Command Mode

Interface Configuration

Command Usage

- The re-authentication process verifies the connected client’s user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked.
- The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

Related Commands

dot1x timeout re-authperiod (25-31)

dot1x timeout quiet-period

This command sets the time that a switch port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form to reset the default.

Syntax

dot1x timeout quiet-period *seconds*
no dot1x timeout quiet-period

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated.

Syntax

dot1x timeout re-authperiod *seconds*
no dot1x timeout re-authperiod

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

dot1x timeout tx-period

This command sets the time that an interface on the switch waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

dot1x timeout tx-period *seconds*
no dot1x timeout tx-period

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

show dot1x

This command shows general port authentication related settings on the switch or a specific interface.

Syntax

show dot1x [**statistics**] [**interface** *interface*]

- **statistics** - Displays dot1x status for each port.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- *Global 802.1X Parameters* – Shows whether or not 802.1X port authentication is globally enabled on the switch.
- *802.1X Port Summary* – Displays the port access control parameters for each interface that has enabled 802.1X, including the following items:
  - Status – Administrative state for port access control.
  - Operation Mode – Allows single or multiple hosts (page 25-29).
  - Mode – Dot1x port control mode (page 25-28).
  - Authorized – Authorization status (yes or n/a - not authorized).

- *802.1X Port Details* – Displays the port access control parameters for each interface, including the following items:
  - reauth-enabled – Periodic re-authentication (page 25-30).
  - reauth-period – Time after which a connected client must be re-authenticated (page 25-31).
  - quiet-period – Time a port waits after Max Request Count is exceeded before attempting to acquire a new client (page 25-31).
  - tx-period – Time a port waits during authentication session before re-transmitting EAP packet (page 25-32).
  - supplicant-timeout – Supplicant timeout.
  - server-timeout – Server timeout.
  - reauth-max – Maximum number of reauthentication attempts.
  - max-req – Maximum number of times a port will retransmit an EAP request/identity packet to the client before it times out the authentication session (page 25-27).
  - Status – Authorization status (authorized or not).
  - Operation Mode – Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
  - Max Count – The maximum number of hosts allowed to access this port (page 25-29).
  - Port-control – Shows the dot1x mode on a port as auto, force-authorized, or force-unauthorized (page 25-28).
  - Supplicant – MAC address of authorized client.
  - Current Identifier – The integer (0-255) used by the Authenticator to identify the current authentication session.
- *Authenticator State Machine*
  - State – Current state (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
  - Reauth Count – Number of times connecting state is re-entered.
- *Backend State Machine*
  - State – Current state (including request, response, success, fail, timeout, idle, initialize).
  - Request Count – Number of EAP Request packets sent to the Supplicant without receiving a response.
  - Identifier(Server) – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
- *Reauthentication State Machine*
  - State – Current state (including initialize, reauthenticate).

Example

```
Console#show dot1x
Global 802.1X Parameters
 system-auth-control: enable

802.1X Port Summary

Port Name  Status           Operation Mode   Mode                  Authorized
1/1         disabled        Single-Host      ForceAuthorized       n/a
1/2         disabled        Single-Host      ForceAuthorized       n/a
:
1/25        disabled        Single-Host      ForceAuthorized       yes
1/26        enabled         Single-Host      Auto                  yes

802.1X Port Details

802.1X is enabled on port 1/1
:
802.1X is enabled on port 26
 Reauth-enabled:         Enabled
 Reauth-period:          3600
 Quiet-period:           60
 TX-period:              30
 Supplicant-timeout:     30
 Server-timeout:         10
 Reauth-max:             2
 Max-req:                2
Status                   Authorized
Operation Mode           Multi-Host
Max count                5
Port-control             Auto
Supplicant                00-e0-29-94-34-65
Current Identifier       3

Authenticator State Machine
State                 Authenticated
Reauth Count         0

Backend State Machine
State                Idle
Request Count        0
Identifier(Server)   2

Reauthentication State Machine
State                 Initialize

Console#
```

Management IP Filter Commands

This section describes commands used to configure IP management access to the switch.

Table 25-14 IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	25-35
show management	Displays the switch to be monitored or configured from a browser	PE	25-36

management

This command specifies the client IP addresses that are allowed management access to the switch through various protocols. Use the **no** form to restore the default setting.

Syntax

[**no**] **management** {**all-client** | **http-client** | **snmp-client** | **telnet-client**} *start-address* [*end-address*]

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- *start-address* - A single IP address, or the starting address of a range.
- *end-address* - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (i.e., SNMP, web or Telnet), the switch will not accept overlapping address ranges. When entering addresses for different groups, the switch will accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.
- You can delete an address range just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

show management

This command displays the client IP addresses that are allowed management access to the switch through various protocols.

Syntax

show management {**all-client** | **http-client** | **snmp-client** | **telnet-client**}

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
 HTTP-Client:
   Start IP address       End IP address
-----------------------------------------------
1. 192.168.1.19           192.168.1.19
2. 192.168.1.25           192.168.1.30

 SNMP-Client:
   Start IP address       End IP address
-----------------------------------------------
1. 192.168.1.19           192.168.1.19
2. 192.168.1.25           192.168.1.30

 TELNET-Client:
   Start IP address      End IP address
-----------------------------------------------
1. 192.168.1.19           192.168.1.19
2. 192.168.1.25           192.168.1.30

Console#
```

Chapter 26: Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IPv4 frames (based on address, protocol, Layer 4 protocol port number or TCP control code), IPv6 frames (based on address, next header type, or flow label), or any frames (based on MAC address or Ethernet type). To filter packets, first create an access list, add the required rules, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 26-1 Access Control List Commands

Command Groups	Function	Page
IPv4 ACLs	Configures ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code	26-1
IPv6 ACLs	Configures ACLs based on IPv6 addresses, next header type, and flow label	26-7
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	26-12
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	26-16

IPv4 ACLs

The commands in this section configure ACLs based on IPv4 addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IPv4 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports

Table 26-2 IPv4 ACL Commands

Command	Function	Mode	Page
access-list ip	Creates an IPv4 ACL and enters configuration mode for standard or extended IPv4 ACLs	GC	26-2
permit, deny	Filters packets matching a specified source IPv4 address	IPv4-STD-ACL	26-2
permit, deny	Filters packets meeting the specified criteria, including source and destination IPv4 address, TCP/UDP port number, protocol type, and TCP control code	IPv4-EXT-ACL	26-3
show ip access-list	Displays the rules for configured IPv4 ACLs	PE	26-5
ip access-group	Adds a port to an IPv4 ACL	IC	26-6
show ip access-group	Shows port assignments for IPv4 ACLs	PE	26-6

access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IPv4 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ip** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny 26-2
ip access-group (26-6)
show ip access-list (26-5)

permit, **deny** (Standard IPv4 ACL)

This command adds a rule to a Standard IPv4 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} {**any** | *source bitmask* | **host** *source*}

- **any** – Any source IP address.
- *source* – Source IP address.
- *bitmask* – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard IPv4 ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (26-2)

permit, **deny** (Extended IPv4 ACL)

This command adds a rule to an Extended IPv4 ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**} [*protocol-number* | **udp**]
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]

[**no**] {**permit** | **deny**} **tcp**
{**any** | *source address-bitmask* | **host** *source*}
{**any** | *destination address-bitmask* | **host** *destination*}
[**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*]
[**source-port** *sport* [*bitmask*]] [**destination-port** *dport* [*port-bitmask*]]
[**control-flag** *control-flags flag-bitmask*]

- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.

- **host** – Keyword followed by a specific IP address.
- *precedence* – IP precedence level. (Range: 0-7)
- *tos* – Type of Service level. (Range: 0-15)
- *dscp* – DSCP priority level. (Range: 0-63)
- *sport* – Protocol[26] source port number. (Range: 0-65535)
- *dport* – Protocol[26] destination port number. (Range: 0-65535)
- *port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)
- *control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *flag-bitmask* – Decimal number representing the code bits to match.

Default Setting

None

Command Mode

Extended IPv4 ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate "match" and 0 bits to indicate "ignore." The bitmask is bitwise ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.
- You can specify both Precedence and ToS in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit "1" means to match a bit and "0" means to ignore a bit. The following bits may be specified:

  - 1 (fin) – Finish
  - 2 (syn) – Synchronize
  - 4 (rst) – Reset
  - 8 (psh) – Push
  - 16 (ack) – Acknowledgement
  - 32 (urg) – Urgent pointer

  For example, use the code value and mask below to catch packets with the following flags set:

  - SYN flag valid, use "control-code 2 2"
  - Both SYN and ACK valid, use "control-code 18 18"
  - SYN valid and ACK invalid, use "control-code 2 18"

[26] Includes TCP, UDP or other protocol types.

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; i.e., the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (i.e., HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
 destination-port 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
 control-flag 2 2
Console(config-ext-acl)#
```

Related Commands

access-list ip (26-2)

show ip access-list

This command displays the rules for configured IPv4 ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IP ACL.
- **extended** – Specifies an extended IP ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ip access-list standard
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
Console#
```

Related Commands

permit, deny 26-2
ip access-group (26-6)

ip access-group

This command binds a port to an IPv4 ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ip access-group** *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

Related Commands

show ip access-list (26-5)

show ip access-group

This command shows the ports assigned to IPv4 ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
 IP standard access-list david
Console#
```

Related Commands

ip access-group (26-6)

IPv6 ACLs

The commands in this section configure ACLs based on IPv6 addresses, next header type, and flow label. To configure IPv6 ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports

Table 26-3 IPv6 ACL Commands

Command	Function	Mode	Page
access-list ipv6	Creates an IPv6 ACL and enters configuration mode for standard or extended IPv6 ACLs	GC	26-7
permit, deny	Filters packets matching a specified source IPv6 address	IPv6-STD-ACL	26-8
permit, deny	Filters packets meeting the specified criteria, including destination IPv6 address, next header type, and flow label	IPv6-EXT-ACL	26-9
show ipv6 access-list	Displays the rules for configured IPv6 ACLs	PE	26-11
ipv6 access-group	Adds a port to an IPv6 ACL	IC	26-11
show ipv6 access-group	Shows port assignments for IPv6 ACLs	PE	26-12

access-list ipv6

This command adds an IP access list and enters configuration mode for standard or extended IPv6 ACLs. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list ipv6** {**standard** | **extended**} *acl_name*

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the destination IP address, and other more specific criteria.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ipv6 standard david
Console(config-std-ipv6-acl)#
```

Related Commands

permit, deny (26-8)
ipv6 access-group (26-11)
show ipv6 access-list (26-11)

permit, **deny** (Standard IPv6 ACL)

This command adds a rule to a Standard IPv6 ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**} {**any** | *source-ipv6-address*[*/prefix-length*] |
host *source-ipv6-address*}

- **any** – Any source IP address.
- *source-ipv6-address* - An IPv6 source address. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- *prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard IPv6 ACL

Command Usage

New rules are appended to the end of the list.

Example

This example configures one permit rule for the specific address 2009:DB9:2229::79 and another rule for the addresses with the network prefix 2009:DB9:2229:5::/64.

```
Console(config-std-ipv6-acl)#permit host 2009:DB9:2229::79
Console(config-std-ipv6-acl)#permit 2009:DB9:2229:5::/64
Console(config-std-ipv6-acl)#
```

Related Commands

access-list ipv6 (26-7)

permit, **deny** (Extended IPv6 ACL)

This command adds a rule to an Extended IPv6 ACL. The rule sets a filter condition for packets with specific destination IP addresses, next header type, or flow label. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit | deny**}
{**any** | *destination-ipv6-address*[*/prefix-length*]}
[**next-header** *next-header*] [**dscp** *dscp*] [**flow-label** *flow-label*]

- **any** – Keyword indicating any IPv6 destination address (an abbreviation for the IPv6 prefix ::/0).
- *destination-ipv6-address* - An IPv6 destination address. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. (The switch only checks the first 64 bits of the destination address.)
- *prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).
- *dscp* – DSCP priority level. (Range: 0-63)
- *flow-label* – A label for packets belonging to a particular traffic “flow” for which the sender requests special handling by IPv6 routers, such as non-default quality of service or “real-time” service (see RFC 2460). (Range: 0-16777215)
- *next-header* – Identifies the type of header immediately following the IPv6 header. (Range: 0-255)

Default Setting

None

Command Mode

Extended IPv6 ACL

Command Usage

- All new rules are appended to the end of the list.
- A flow label is assigned to a flow by the flow's source node. New flow labels must be chosen pseudo-randomly and uniformly from the range 1 to FFFFF hexadecimal. The purpose of the random allocation is to make any set of bits within the Flow Label field suitable for use as a hash key by routers, for looking up the state associated with the flow.

  A flow identifies a sequence of packets sent from a particular source to a particular (unicast or multicast) destination for which the source desires special handling by the intervening routers. The nature of that special handling might be conveyed to the routers by a control protocol, such as a resource reservation protocol, or by information within the flow's packets themselves, e.g., in a hop-by-hop option. A flow is uniquely identified by the combination of a source address and a non-zero flow label. Packets that do not belong to a flow carry a flow label of zero.

Hosts or routers that do not support the functions specified by the flow label must set the field to zero when originating a packet, pass the field on unchanged when forwarding a packet, and ignore the field when receiving a packet.

- Optional internet-layer information is encoded in separate headers that may be placed between the IPv6 header and the upper-layer header in a packet. There are a small number of such extension headers, each identified by a distinct Next Header value. IPv6 supports the values defined for the IPv4 Protocol field in RFC 1700, including these commonly used headers:

0	:	Hop-by-Hop Options	(RFC 2460)
6	:	TCP Upper-layer Header	(RFC 1700)
17	:	UDP Upper-layer Header	(RFC 1700)
43	:	Routing	(RFC 2460)
44	:	Fragment	(RFC 2460)
51	:	Authentication	(RFC 2402)
50	:	Encapsulating Security Payload	(RFC 2406)
60	:	Destination Options	(RFC 2460)

Example

This example accepts any incoming packets if the destination address is 2009:DB9:2229::79/48.

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48
Console(config-ext-ipv6-acl)#
```

This allows packets to any destination address when the DSCP value is 5.

```
Console(config-ext-ipv6-acl)#permit any dscp 5
Console(config-ext-ipv6-acl)#
```

This allows any packets sent to the destination 2009:DB9:2229::79/48 when the flow label is 43."

```
Console(config-ext-ipv6-acl)#permit 2009:DB9:2229::79/48 flow-label 43
Console(config-ext-ipv6-acl)#
```

Related Commands

access-list ipv6 (26-7)

show ipv6 access-list

This command displays the rules for configured IPv6 ACLs.

Syntax

show ip access-list {**standard** | **extended**} [*acl_name*]

- **standard** – Specifies a standard IPv6 ACL.
- **extended** – Specifies an extended IPv6 ACL.
- *acl_name* – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show ipv6 access-list standard
IPv6 standard access-list david:
  permit host 2009:DB9:2229::79
  permit 2009:DB9:2229:5::/64
Console#
```

Related Commands

permit, deny (26-8)
ipv6 access-group (26-11)

ipv6 access-group

This command binds a port to an IPv6 ACL. Use the **no** form to remove the port.

Syntax

[**no**] **ipv6 access-group** *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.
- IPv6 ACLs can only be applied to ingress packets.

Example

```
Console(config)#int eth 1/2
Console(config-if)#ipv6 access-group standard david in
Console(config-if)#
```

Related Commands

show ipv6 access-list (26-11)

show ipv6 access-group

This command shows the ports assigned to IPv6 ACLs.

Command Mode

Privileged Exec

Example

```
Console#show ip access-group
Interface ethernet 1/2
 IPv6 standard access-list david in
Console#
```

Related Commands

ipv6 access-group (26-11)

MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, and then bind the access list to one or more ports

Table 26-4 MAC ACL Commands

Command	Function	Mode	Page
access-list mac	Creates a MAC ACL and enters configuration mode	GC	26-12
permit, deny	Filters packets matching a specified source and destination address, packet format, and Ethernet type	MAC-ACL	26-13
show mac access-list	Displays the rules for configured MAC ACLs	PE	26-15
mac access-group	Adds a port to a MAC ACL	IC	26-15
show mac access-group	Shows port assignments for MAC ACLs	PE	26-16

access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

Syntax

[**no**] **access-list mac** *acl_name*

acl_name – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- When you create a new ACL or enter configuration mode for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, you must add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

Related Commands

permit, deny (26-13)
mac access-group (26-15)
show mac access-list (26-15)

permit, **deny** (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (i.e., physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

Syntax

[**no**] {**permit** | **deny**}
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

Note:- The default is for Ethernet II packets.

[**no**] {**permit** | **deny**} **tagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*] [**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **untagged-eth2**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**ethertype** *protocol* [*protocol-bitmask*]]

[**no**] {**permit** | **deny**} **tagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}
[**vid** *vid vid-bitmask*]

[**no**] {**permit** | **deny**} **untagged-802.3**
{**any** | **host** *source* | *source address-bitmask*}
{**any** | **host** *destination* | *destination address-bitmask*}

- **tagged-eth2** – Tagged Ethernet II packets.
- **untagged-eth2** – Untagged Ethernet II packets.
- **tagged-802.3** – Tagged Ethernet 802.3 packets.
- **untagged-802.3** – Untagged Ethernet 802.3 packets.
- **any** – Any MAC source or destination address.
- **host** – A specific MAC address.
- *source* – Source MAC address.
- *destination* – Destination MAC address range with bitmask.
- *address-bitmask*[27] – Bitmask for MAC address (in hexidecimal format).
- vid – VLAN ID. (Range: 1-4093)
- *vid-bitmask*[27] – VLAN bitmask. (Range: 1-4093)
- *protocol* – A specific Ethernet protocol number. (Range: 600-fff hex.)
- *protocol-bitmask*[27] – Protocol bitmask. (Range: 600-fff hex.)

Default Setting

None

Command Mode

MAC ACL

Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype 0800
Console(config-mac-acl)#
```

Related Commands

access-list mac (26-12)

[27] For all bitmasks, “1” means care and “0” means ignore.

show mac access-list

This command displays the rules for configured MAC ACLs.

Syntax

show mac access-list [*acl_name*]

acl_name – Name of the ACL. (Maximum length: 16 characters)

Command Mode

Privileged Exec

Example

```
Console#show mac access-list
MAC access-list jerry:
  permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

Related Commands

permit, deny 26-13
mac access-group (26-15)

mac access-group

This command binds a port to a MAC ACL. Use the **no** form to remove the port.

Syntax

mac access-group *acl_name* **in**

- *acl_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.

Default Setting

None

Command Mode

Interface Configuration (Ethernet)

Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and you bind it to a different ACL, the switch will replace the old binding with the new one.

Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

Related Commands

show mac access-list (26-15)

show mac access-group

This command shows the ports assigned to MAC ACLs.

Command Mode

Privileged Exec

Example

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 in
Console#
```

Related Commands

mac access-group (26-15)

ACL Information

This section describes commands used to display ACL information.

Table 26-5 ACL Information Commands

Command	Function	Mode	Page
show access-list	Show all IPv4 ACLs and associated rules	PE	26-16
show access-group	Shows the IPv4 ACLs assigned to each port	PE	26-17

show access-list

This command shows all IPv4 ACLs and associated rules.

Command Mode

Privileged Exec

Example

```
Console#show access-list
IP standard access-list david:
  permit host 10.1.1.21
  permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
  permit 10.7.1.1 255.255.255.0 any
  permit 192.168.1.0 255.255.255.0 any destination-port 80 80
  permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
  permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
  deny tcp any any control-flag 2 2
  permit any any
Console#
```

show access-group

This command shows the port assignments of IPv4 ACLs.

Command Mode

Privileged Executive

Example

```
Console#show access-group
Interface ethernet 1/2
 IP standard access-list david
 MAC access-list jerry
Console#
```

Chapter 27: Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Table 27-1 Interface Commands

Command	Function	Mode	Page
interface	Configures an interface type and enters interface configuration mode	GC	27-1
description	Adds a description to an interface configuration	IC	27-2
speed-duplex	Configures the speed and duplex operation of a given interface when autonegotiation is disabled	IC	27-3
negotiation	Enables autonegotiation of a given interface	IC	27-4
capabilities	Advertises the capabilities of a given interface for use in autonegotiation	IC	27-4
flowcontrol	Enables flow control on a given interface	IC	27-5
media-type	Force port type selected for combination ports	IC	27-6
shutdown	Disables an interface	IC	27-7
switchport broadcast packet-rate	Configures the broadcast storm control threshold	IC	27-7
clear counters	Clears statistics on an interface	PE	27-8
show interfaces status	Displays status for the specified interface	NE, PE	27-9
show interfaces counters	Displays statistics for the specified interfaces	NE, PE	27-10
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	27-11

interface

This command configures an interface type and enter interface configuration mode. Use the **no** form with a trunk to remove an inactive interface.

Syntax

interface *interface*
no interface port-channel *channel-id*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

None

Command Mode

Global Configuration

Example

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

description

This command adds a description to an interface. Use the **no** form to remove the description.

Syntax

description *string*
no description

string - Comment or a description to help you remember what is attached to this interface. (Range: 1-64 characters)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The description is displayed by the **show interfaces status** command (page 27-9) and in the running-configuration file. An example of the value which a network manager might store in this object is the name of the manufacturer, and the product name.

Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

Syntax

speed-duplex {**10000full** | **1000full** | **100full** | **100half** | **10full** | **10half**}
no speed-duplex

- **10000full** - Forces 10 Gbps full-duplex operation
- **1000full** - Forces 1 Gbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

Default Setting

- Auto-negotiation is enabled by default.
- When auto-negotiation is disabled, the default speed-duplex setting is:
  - Gigabit Ethernet ports – **1000full** (1 Gbps full-duplex)
  - 10 Gigabit Ethernet ports – **10000full** (10 Gbps full-duplex)

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The 1000BASE-T and 10GBASE-T standards do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T or 10GBASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.
- To force operation to the speed and duplex mode specified in a **speed-duplex** command, use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed/duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (27-4)
capabilities (27-4)

negotiation

This command enables autonegotiation for a given interface. Use the **no** form to disable autonegotiation.

Syntax

[**no**] **negotiation**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- 1000BASE-T and 10GBASE-T do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T or 10GBASE-T port or trunk.
- When auto-negotiation is enabled the switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.
- If autonegotiation is disabled, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ-45 ports.

Example

The following example configures port 11 to use autonegotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

Related Commands

capabilities (27-4)
speed-duplex (27-3)

capabilities

This command advertises the port capabilities of a given interface during autonegotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

Syntax

[**no**] **capabilities** {**10000full** | **1000full** | **100full** | **100half** | **10full** | **10half** | **flowcontrol** | **symmetric**}

- **10000full** - Supports 10 Gbps full-duplex operation
- **1000full** - Supports 1 Gbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation

- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (*The current switch ASIC only supports symmetric pause frames for 1 Gbps connections.*)

Default Setting

- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-SX/LX/LH (SFP): 1000full
- 10GBASE-SR/LR/ER (XFP): 10000full

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- 1000BASE-T and 10GBASE-T do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T or 10GBASE-T port or trunk.
- When auto-negotiation is enabled with the **negotiation** command, the switch will negotiate the best settings for a link based on the **capabilites** command. When auto-negotiation is disabled, you must manually specify the link attributes with the **speed-duplex** and **flowcontrol** commands.

Example

The following example configures Ethernet port 5 capabilities to 100half and 100full.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#
```

Related Commands

negotiation (27-4)
speed-duplex (27-3)
flowcontrol (27-5)

flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

Syntax

[**no**] **flowcontrol**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- 1000BASE-T and 10GBASE-T do not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T or 10GBASE-T port or trunk.
- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.
- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface.
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

Related Commands

negotiation (27-4)
capabilities (flowcontrol, symmetric) (27-4)

media-type

This command forces the port type selected for combination ports 21-24/45-48. Use the **no** form to restore the default mode.

Syntax

media-type *mode*
no media-type

- *mode*
  - **copper-forced** - Always uses the built-in RJ-45 port.
  - **sfp-forced** - Always uses the SFP port (even if module not installed).
  - **sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

Default Setting

sfp-preferred-auto

Command Mode

Interface Configuration (Ethernet - Ports 21-24/45-48)

Example

This forces the switch to use the built-in RJ-45 port for the combination port 48.

```
Console(config)#interface ethernet 1/48
Console(config-if)#media-type copper-forced
Console(config-if)#
```

shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

Syntax

[**no**] **shutdown**

Default Setting

All interfaces are enabled.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This command allows you to disable a port due to abnormal behavior (e.g., excessive collisions), and then reenable it after the problem has been resolved. You may also want to disable a port for security reasons.

Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

switchport broadcast packet-rate

This command configures broadcast storm control. Use the **no** form to disable broadcast storm control.

Syntax

switchport broadcast packet-rate *rate*
no switchport broadcast

rate - Threshold level as a rate; i.e., packets per second. (Range: 500-262143)

Default Setting

Enabled for all ports
Packet-rate limit: 500 pps

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- Broadcast control does not effect IP multicast traffic.

Example

The following shows how to configure broadcast storm control at 600 packets per second:

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

clear counters

This command clears statistics on an interface.

Syntax

clear counters *interface*

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, if you log out and back into the management interface, the statistics displayed will show the absolute value accumulated since the last power reset.

Example

The following example clears statistics on port 5.

```
Console#clear counters ethernet 1/5
Console#
```

show interfaces status

This command displays the status for an interface.

Syntax

show interfaces status [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)
- **vlan** *vlan-id* (Range: 1-4093)

Default Setting

Shows the status for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Displaying Connection Status” on page 8-1.

Example

```
Console#show interfaces status ethernet 1/5
Information of Eth 1/5
 Basic Information:
  Port Type              : 1000T
  Mac Address            : 12-34-12-34-12-49
 Configuration:
  Name                   :
  Port Admin             : Up
  Speed-duplex           : Auto
  Capabilities           : 10half, 10full, 100half, 100full, 1000full
  Broadcast Storm        : Enabled
  Broadcast Storm Limit  : 500 packets/second
  Flow Control           : Disabled
  LACP                   : Disabled
  Port Security          : Disabled
  Max MAC Count          : 0
  Port Security Action   : None
  Media Type             : Copper forced
Current status:
  Link Status            : Up
  Port Operation Status  : Up
  Operation Speed-duplex : 100full
  Flow Control Type      : None
Console#show interfaces status vlan 1
 Information of VLAN 1
 MAC Address:              00-00-AB-CD-00-00
Console#
```

show interfaces counters

This command displays interface statistics.

Syntax

show interfaces counters [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows the counters for all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed. For a description of the items displayed by this command, see “Showing Port Statistics” on page 8-22.

Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
 Iftable Stats:
  Octets Input: 30658, Octets Output: 196550
  Unicast Input: 6, Unicast Output: 5
  Discard Input: 0, Discard Output: 0
  Error Input: 0, Error Output: 0
  Unknown Protos Input: 0, QLen Output: 0
 Extended iftable Stats:
  Multi-cast input: 0, Multi-cast output: 3064
  Broadcast input: 262, Broadcast output: 1
 Ether-like Stats:
  Alignment Errors: 0, FCS Errors: 0
  Single Collision Frames: 0, Multiple Collision Frames: 0
  SQE Test Errors: 0, Deferred Transmissions: 0
  Late Collisions: 0, Excessive Collisions: 0
  Internal Mac Transmit Errors: 0, Internal Mac Receive Errors: 0
  Frames Too Long: 0, Carrier Sense Errors: 0
  In Pause Frames: 0, Out Pause Frames: 0
  Symbol Errors: 0
 RMON stats:
  Drop Events: 0, Octets: 227208, Packets: 3338
  Broadcast Pkts: 263, Multi-cast Pkts: 3064
  Undersize Pkts: 0, Oversize Pkts: 0
  Fragments: 0, Jabbers: 0
  CRC Align Errors: 0, Collisions: 0
  Packet Size <= 64 octets: 3150, Packet Size 65 to 127 octets: 139
  Packet Size 128 to 255 octets: 49, Packet Size 256 to 511 octets: 0
  Packet Size 512 to 1023 octets: 0, Packet Size 1024 to 1518 octets: 0
Console#
```

show interfaces switchport

This command displays the administrative and operational status of the specified interfaces.

Syntax

show interfaces switchport [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows all interfaces.

Command Mode

Normal Exec, Privileged Exec

Command Usage

If no interface is specified, information on all interfaces is displayed.

Example

This example shows the configuration setting for port 4.

```
Console#show interfaces switchport ethernet 1/4
 Broadcast Threshold              : Enabled, 500 packets/second
 LACP Status                    : Disabled
 Ingress Rate Limit               : Disable, 1000M bits per second
 Egress Rate Limit                : Disable, 1000M bits per second
 VLAN Membership Mode           : Hybrid
 Ingress Rule                   : Disabled
 Acceptable Frame Type          : All frames
 Native VLAN                   : 1
 Priority for Untagged Traffic : 0
 GVRP Status                    : Disabled
 Allowed VLAN                   : 1(u),
 Forbidden VLAN                :
 802.1Q-tunnel Status:           Disable
 802.1Q-tunnel Mode:             NORMAL
 802.1Q-tunnel TPID:             8100(Hex)
Console#
```

Table 27-2 show interfaces switchport - display description

Field	Description
Broadcast Threshold	Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (page 27-7).
LACP Status	Shows if Link Aggregation Control Protocol has been enabled or disabled (page 28-3).
Ingress/Egress Rate Limit	Shows if rate limiting is enabled, and the current rate limit (page 30-1).
VLAN Membership Mode	Indicates membership mode as Trunk or Hybrid (page 34-8).

Table 27-2 show interfaces switchport - display description (Continued)

Field	Description
Ingress Rule	Shows if ingress filtering is enabled or disabled (page 34-9).
Acceptable Fame Type	Shows if acceptable VLAN frames include all types or tagged frames only (page 34-9).
Native VLAN	Indicates the default Port VLAN ID (page 34-10).
Priority for Untagged Traffic	Indicates the default priority for untagged frames (page 35-3).
GVRP Status	Shows if GARP VLAN Registration Protocol is enabled or disabled (page 34-3).
Allowed VLAN	Shows the VLANs this interface has joined, where “(u)” indicates untagged and “(t)” indicates tagged (page 34-11).
Forbidden VLAN	Shows the VLANs this interface can not dynamically join via GVRP (page 34-12).
802.1Q-tunnel Status	Shows if 802.1Q tunnel is enabled on this interface (page 34-15).
802.1Q-tunnel Mode	Shows the tunnel mode as Normal, 802.1Q Tunnel or 802.1Q Tunnel Uplink (page 34-15).
802.1Q-tunnel TPID	Shows the Tag Protocol Identifier used for learning and switching packets (page 34-16).

Chapter 28: Link Aggregation Commands

Ports can be statically grouped into an aggregate link (i.e., trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or you can use the Link Aggregation Control Protocol (LACP) to automatically negotiate a trunk link between this switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. This switch supports up to 12 trunks, and up to 32 for the stack. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 28-1 Link Aggregation Commands

Command	Function	Mode	Page
Manual Configuration Commands			
interface port-channel	Configures a trunk and enters interface configuration mode for the trunk	GC	27-1
channel-group	Adds a port to a trunk	IC (Ethernet)	28-2
Dynamic Configuration Commands			
lacp	Configures LACP for the current interface	IC (Ethernet)	28-3
lacp system-priority	Configures a port's LACP system priority	IC (Ethernet)	28-4
lacp admin-key	Configures a port's administration key	IC (Ethernet)	28-5
lacp admin-key	Configures an port channel's administration key	IC (Port Channel)	28-6
lacp port-priority	Configures a port's LACP port priority	IC (Ethernet)	28-6
Trunk Status Display Commands			
show interfaces status port-channel	Shows trunk information	NE, PE	27-9
show lacp	Shows LACP information	PE	28-7

Guidelines for Creating Trunks

General Guidelines –

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to 8 ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (i.e., speed and duplex mode), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN via the specified port-channel.

- STP, VLAN, and IGMP settings can only be made for the entire trunk via the specified port-channel.

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).
- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

channel-group

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

Syntax

channel-group *channel-id*
no channel-group

channel-id - Trunk index (Range: 1-32)

Default Setting

The current port will be added to this trunk.

Command Mode

Interface Configuration (Ethernet)

Command Usage

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the switch.

Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

lacp

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

Syntax

[**no**] **lacp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

Example

The following shows LACP enabled on ports 10-12. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
 Basic Information:
  Port Type             : 100TX
  Mac Address           : 12-34-12-34-12-3F
Configuration:
  Name                  :
  Port Admin            : Up
  Speed-duplex          : Auto
  Capabilities          : 10half, 10full, 100half, 100full
  Flow Control          : Disabled
  Port Security         : Disabled
  Max MAC Count         : 0
 Current status:
  Created By             : LACP
  Link Status            : Up
  Port Operation Status  : Up
  Operation speed-duplex : 100full
  Flow control Type      : None
  Member Ports             : Eth1/10, Eth1/11, Eth1/12,
Console#
```

lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **system-priority** *priority*
no lacp {**actor** | **partner**} **system-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the switch’s MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **admin-key** *key*
[**no**] **lacp** {**actor** | **partner**} **admin-key**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

Syntax

lacp admin-key *key*
[**no**] **lacp admin-key**

key - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on this switch. (Range: 0-65535)

Default Setting

0

Command Mode

Interface Configuration (Port Channel)

Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (i.e., it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

Syntax

lacp {**actor** | **partner**} **port-priority** *priority*
no lacp {**actor** | **partner**} **port-priority**

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *priority* - LACP port priority is used to select a backup link. (Range: 0-65535)

Default Setting

32768

Command Mode

Interface Configuration (Ethernet)

Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

show lacp

This command displays LACP information.

Syntax

show lacp [*port-channel*] {**counters** | **internal** | **neighbors** | **sys-id**}

- *port-channel* - Local identifier for a link aggregation group. (Range: 1-32)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- **neighbors** - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

Default Setting

Port Channel: all

Command Mode

Privileged Exec

Example

```
Console#show lacp 1 counters
Port Channel: 1
-------------------------------------------------------------------------
Eth 1/ 2
-------------------------------------------------------------------------
  LACPDUs Sent          : 12
  LACPDUs Receive       : 6
  Marker Sent           : 0
  Marker Receive        : 0
  LACPDUs Unknown Pkts : 0
  LACPDUs Illegal Pkts : 0
⋮
```

Table 28-2 show lacp counters - display description

Field	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received on this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
LACPDUs Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
LACPDUs Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

```
Console#show lacp 1 internal
Port Channel : 1
-------------------------------------------------------------------------
Oper Key   : 3
Admin Key : 0
Eth 1/ 1
-------------------------------------------------------------------------
  LACPDUs Internal       : 30 seconds
  LACP System Priority : 32768
  LACP Port Priority     : 32768
  Admin Key              : 3
  Oper Key               : 3
  Admin State               : defaulted, aggregation, long timeout, LACP-activity
  Oper State               : distributing, collecting, synchronization, aggregation,
                          long timeout, LACP-activity
⋮
```

Table 28-3 show lacp internal - display description

Field	Description
Oper Key	Current operational value of the key for the aggregation port.
Admin Key	Current administrative value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.
LACP System Priority	LACP system priority assigned to this port channel.

Table 28-3 show lacp internal - display description (Continued)

Field	Description
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; i.e., distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; i.e., collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; i.e., it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; i.e., a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

```
Console#show lacp 1 neighbors
Port Channel 1 neighbors
-------------------------------------------------------------------------
Eth 1/ 1
-------------------------------------------------------------------------
  Partner Admin System ID      :    32768, 00-00-00-00-00-00
  Partner Oper System ID        : 32768, 00-12-CF-61-24-2F
  Partner Admin Port Number : 1
  Partner Oper Port Number  : 1
  Port Admin Priority          : 32768
  Port Oper Priority           : 32768
  Admin Key                   : 0
  Oper  Key                   :  3
  Admin State:                      defaulted, distributing, collecting,
                               synchronization,  long timeout,
  Oper State:                       distributing, collecting, synchronization,
                               aggregation,  long  timeout, LACP-activity
⋮
```

Table 28-4 show lacp neighbors - display description

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.

Table 28-4 show lacp neighbors - display description (Continued)

Field	Description
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner’s state parameters. (See preceding table.)
Oper State	Operational values of the partner’s state parameters. (See preceding table.)

```
Console#show lacp sysid
Port Channel       System Priority     System MAC Address
------------------------------------------------------------------------------
             1                32768      00-30-F1-8F-2C-A7
             2                32768      00-30-F1-8F-2C-A7
             3                32768      00-30-F1-8F-2C-A7
             4                32768      00-30-F1-8F-2C-A7
             5                32768      00-30-F1-8F-2C-A7
             6                32768      00-30-F1-8F-2C-A7
             7                32768      00-30-F1-D4-73-A0
             8                32768      00-30-F1-D4-73-A0
             9                32768      00-30-F1-D4-73-A0
            10                32768      00-30-F1-D4-73-A0
            11                32768      00-30-F1-D4-73-A0
            12                32768      00-30-F1-D4-73-A0
⋮
```

Table 28-5 show lacp sysid - display description

Field	Description
Channel group	A link aggregation group configured on this switch.
System Priority*	LACP system priority for this channel group.
System MAC Address*	System MAC address.

* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

Chapter 29: Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Table 29-1 Mirror Port Commands

Command	Function	Mode	Page
port monitor	Configures a mirror session	IC	29-1
show port monitor	Shows the configuration for a mirror port	PE	29-2

port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

Syntax

port monitor *interface* [**rx** | **tx** | **both**]
no port monitor *interface*

- *interface* - **ethernet** *unit*/*port* (source port)
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

Command Mode

Interface Configuration (Ethernet, destination port)

Command Usage

- You can mirror traffic from any source port to a destination port for real-time analysis. You can then attach a logic analyzer or RMON probe to the destination port and study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- You can create multiple mirror sessions, but all sessions must share the same destination port. However, you should avoid sending too much traffic to the destination port from multiple source ports.

Example

The following example configures the switch to mirror all packets from port 6 to 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

show port monitor

This command displays mirror information.

Syntax

show port monitor [*interface*]

interface - **ethernet** *unit*/*port* (source port)

- *unit* - Stack unit. (Range: 1-8)
- *port* - Port number. (Range: 1-26/50)

Default Setting

Shows all sessions.

Command Mode

Privileged Exec

Command Usage

This command displays the currently configured source port, destination port, and mirror mode (i.e., RX, TX, RX/TX).

Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring
-------------------------------------
 Destination port(listen port):Eth1/1
 Source port(monitored port)  :Eth1/6
 Mode                         :RX/TX
Console#
```

Chapter 30: Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped.

Table 30-1 Rate Limit Commands

Command	Function	Mode	Page
rate-limit	Configures the maximum input or output rate for a port	IC	30-1

rate-limit

This command defines the rate limit for a specific interface. Use this command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

Syntax

rate-limit {**input** | **output**} [*rate*]
no rate-limit {**input** | **output**}

- **input** – Input rate
- **output** – Output rate
- *rate* – Maximum value in Kbps.
  (Range: 1-10000 Mbps for Gigabit Ethernet ports)

Default Setting

Gigabit Ethernet: 1000 Mbps

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Rate limits are not supported for the 10 Gigabit Ethernet ports.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 600
Console(config-if)#
```

Related Command

show interfaces switchport (27-11)

Chapter 31: Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

Table 31-1 Address Table Commands

Command	Function	Mode	Page
mac-address-table static	Maps a static address to a port in a VLAN	GC	31-1
clear mac-address-table dynamic	Removes any learned entries from the forwarding database	PE	31-2
show mac-address-table	Displays entries in the bridge-forwarding database	PE	31-3
mac-address-table aging-time	Sets the aging time of the address table	GC	31-4
show mac-address-table aging-time	Shows the aging time for the address table	PE	31-4

mac-address-table static

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

Syntax

mac-address-table static *mac-address* **interface** *interface* **vlan** *vlan-id* [*action*]

no mac-address-table static *mac-address* **vlan** *vlan-id*

- *mac-address* - MAC address.
- *interface*
  - **ethernet** *unit/port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)
- *vlan-id* - VLAN ID (Range: 1-4093)
- *action* -
  - **delete-on-reset** - Assignment lasts until the switch is reset.
  - **permanent** - Assignment is permanent.

Default Setting

No static addresses are defined. The default mode is **permanent**.

Command Mode

Global Configuration

Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
 ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

Related Commands

ipv6 neighbor (41-26)

clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#clear mac-address-table dynamic
Console#
```

show mac-address-table

This command shows classes of entries in the bridge-forwarding database.

Syntax

show mac-address-table [**address** *mac-address* [*mask*]] [**interface** *interface*] [**vlan** *vlan-id*] [**sort** {**address** | **vlan** | **interface**}]

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)
- *vlan-id* - VLAN ID (Range: 1-4093)
- **sort** - Sort by address, vlan or interface.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - Learned - Dynamic address entries
  - Permanent - Static entry
  - Delete-on-reset - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form xx-xx-xx-xx-xx-xx that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of 00-00-00-00-00-00 means an exact match, and a mask of FF-FF-FF-FF-FF-FF means “any.”
- The maximum number of address entries is 8191.

Example

```
Console#show mac-address-table
 Interface MAC Address       VLAN Type
 --------- ----------------- ---- -----------------
  Eth 1/ 1 00-e0-29-94-34-de    1 Delete-on-reset
Console#
```

Related Commands

show ipv6 neighbors (41-30)

mac-address-table aging-time

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

Syntax

mac-address-table aging-time *seconds*
no mac-address-table aging-time

seconds - Aging time. (Range: 10-1000000 seconds; 0 to disable aging)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The aging time is used to age out dynamically learned forwarding information.

Example

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

show mac-address-table aging-time

This command shows the aging time for entries in the address table.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show mac-address-table aging-time
 Aging time: 300 sec.
Console#
```

Chapter 32: LLDP Commands

Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1ab standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

Table 32-1 LLDP Commands

Command	Function	Mode	Page
lldp	Enables LLDP globally on the switch	GC	32-2
lldp holdtime-multiplier	Configures the time-to-live (TTL) value sent in LLDP advertisements	GC	32-3
lldp notification-interval	Configures the allowed interval for sending SNMP notifications about LLDP changes	GC	32-3
lldp refresh-interval	Configures the periodic transmit interval for LLDP advertisements	GC	32-4
lldp reinit-delay	Configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down	GC	32-5
lldp tx-delay	Configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables	GC	32-5
lldp admin-status	Enables LLDP transmit, receive, or transmit and receive mode on the specified port	IC	32-6
lldp notification	Enables the transmission of SNMP trap notifications about LLDP changes	IC	32-6
lldp basic-tlv management-ip-address	Configures an LLDP-enabled port to advertise the management address for this device	IC	32-7
lldp basic-tlv port-description	Configures an LLDP-enabled port to advertise its port description	IC	32-8
lldp basic-tlv system-capabilities	Configures an LLDP-enabled port to advertise its system capabilities	IC	32-8
lldp basic-tlv system-description	Configures an LLDP-enabled port to advertise the system description	IC	32-9
lldp basic-tlv system-name	Configures an LLDP-enabled port to advertise its system name	IC	32-9
lldp dot1-tlv proto-ident*	Configures an LLDP-enabled port to advertise the supported protocols	IC	32-10
lldp dot1-tlv proto-vid*	Configures an LLDP-enabled port to advertise port related VLAN information	IC	32-10
lldp dot1-tlv pvid*	Configures an LLDP-enabled port to advertise its default VLAN ID	IC	32-11

Table 32-1 LLDP Commands (Continued)

Command	Function	Mode	Page
lldp dot1-tlv vlan-name*	Configures an LLDP-enabled port to advertise its VLAN name	IC	32-11
lldp dot3-tlv link-agg	Configures an LLDP-enabled port to advertise its link aggregation capabilities	IC	32-12
lldp dot3-tlv mac-phy	Configures an LLDP-enabled port to advertise its MAC and physical layer specifications	IC	32-12
lldp dot3-tlv max-frame	Configures an LLDP-enabled port to advertise its maximum frame size	IC	32-13
lldp dot3-tlv poe	Configures an LLDP-enabled port to advertise its Power-over-Ethernet capabilities	IC	32-13
show lldp config	Shows LLDP configuration settings for all ports	PE	32-14
show lldp info local-device	Shows LLDP global and interface-specific configuration settings for this device	PE	32-15
show lldp info remote-device	Shows LLDP global and interface-specific configuration settings for remote devices	PE	32-16
show lldp info statistics	Shows statistical counters for all LLDP-enabled interfaces	PE	32-18

* Vendor-specific options may or may not be advertised by neighboring devices.

lldp

This command enables LLDP globally on the switch. Use the **no** form to disable LLDP.

Syntax

[**no**] **lldp**

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#lldp
Console(config)#
```

lldp holdtime-multiplier

This command configures the time-to-live (TTL) value sent in LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp holdtime-multiplier *value*
no lldp holdtime-multiplier

value - Calculates the TTL in seconds based on (holdtime-multiplier * refresh-interval) ″ 65536 (Range: 2 - 10)

Default Setting

Holdtime multiplier: 4
TTL: 4*30 = 120 seconds

Command Mode

Global Configuration

Command Usage

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

Example

```
Console(config)#lldp holdtime-multiplier 10
Console(config)#
```

lldp notification-interval

This command configures the allowed interval for sending SNMP notifications about LLDP MIB changes. Use the **no** form to restore the default setting.

Syntax

lldp notification-interval *seconds*
no lldp notification-interval

seconds - Specifies the periodic interval at which SNMP notifications are sent. (Range: 5 - 3600 seconds)

Default Setting

5 seconds

Command Mode

Global Configuration

Command Usage

- This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management.
- Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#lldp notification-interval 30
Console(config)#
```

lldp refresh-interval

This command configures the periodic transmit interval for LLDP advertisements. Use the **no** form to restore the default setting.

Syntax

lldp refresh-interval *seconds*
no lldp refresh-delay

seconds - Specifies the periodic interval at which LLDP advertisements are sent. (Range: 5 - 32768 seconds)

Default Setting

30 seconds

Command Mode

Global Configuration

Command Usage

This attribute must comply with the following rule:
(refresh-interval * holdtime-multiplier) ″ 65536

Example

```
Console(config)#lldp refresh-interval 60
Console(config)#
```

lldp reinit-delay

This command configures the delay before attempting to re-initialize after LLDP ports are disabled or the link goes down. Use the **no** form to restore the default setting.

Syntax

lldp reinit-delay *seconds*
no lldp reinit-delay

seconds - Specifies the delay before attempting to re-initialize LLDP. (Range: 1 - 10 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.

Example

```
Console(config)#lldp reinit-delay 10
Console(config)#
```

lldp tx-delay

This command configures a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. Use the **no** form to restore the default setting.

Syntax

lldp tx-delay *seconds*
no lldp tx-delay

seconds - Specifies the transmit delay. (Range: 1 - 8192 seconds)

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

- The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.

- This attribute must comply with the following rule:

  (4 * tx-delay) ″ refresh-interval

Example

```
Console(config)#lldp tx-delay 10
Console(config)#
```

lldp admin-status

This command enables LLDP transmit, receive, or transmit and receive mode on the specified port. Use the **no** form to disable this feature.

Syntax

lldp admin-status {**rx-only** | **tx-only** | **tx-rx**}
no lldp admin-status

- **rx-only** - Only receive LLDP PDUs.
- **tx-only** - Only transmit LLDP PDUs.
- **tx-rx** - Both transmit and receive LLDP Protocol Data Units (PDUs).

Default Setting

tx-rx

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp admin-status rx-only
Console(config-if)#
```

lldp notification

This command enables the transmission of SNMP trap notifications about LLDP changes. Use the **no** form to disable LLDP notifications.

Syntax

[**no**] **lldp notification**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This option sends out SNMP trap notifications to designated target stations at the interval specified by the **lldp notification-interval** command (page 32-3). Trap notifications include information about state changes in the LLDP MIB (IEEE 802.1AB), or organization-specific LLDP-EXT-DOT1 and LLDP-EXT-DOT3 MIBs.
- SNMP trap destinations are defined using the **snmp-server host** command (page 24-5).
- Information about additional changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a trap notification are included in the transmission. An SNMP agent should therefore periodically check the value of lldpStatsRemTableLastChangeTime to detect any lldpRemTablesChange notification-events missed due to throttling or transmission loss.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp notification
Console(config-if)#
```

lldp basic-tlv management-ip-address

This command configures an LLDP-enabled port to advertise the management address for this device. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv management-ip-address**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The management address protocol packet includes the IPv4 address of the switch. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- The management address TLV may also include information about the specific interface associated with this address, and an object identifier indicating the type of hardware component or protocol entity associated with this address. The interface number and OID are included to assist SNMP applications to perform network discovery by indicating enterprise specific or other starting points for the search, such as the Interface or Entity MIB.
- Since there are typically a number of different addresses associated with a Layer 3 device, an individual LLDP PDU may contain more than one management address TLV.

- Every management address TLV that reports an address that is accessible on a port and protocol VLAN through the particular port should be accompanied by a port and protocol VLAN TLV that indicates the VLAN identifier (VID) associated with the management address reported by this TLV.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv management-ip-address
Console(config-if)#
```

lldp basic-tlv port-description

This command configures an LLDP-enabled port to advertise its port description. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv port-description**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The port description is taken from the ifDescr object in RFC 2863, which includes information about the manufacturer, the product name, and the version of the interface hardware/software.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv port-description
Console(config-if)#
```

lldp basic-tlv system-capabilities

This command configures an LLDP-enabled port to advertise its system capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv system-capabilities**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system capabilities identifies the primary function(s) of the system and whether or not these primary functions are enabled. The information advertised by this TLV is described in IEEE 802.1AB.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-capabilities
Console(config-if)#
```

lldp basic-tlv system-description

This command configures an LLDP-enabled port to advertise the system description. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv system-description**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system description is taken from the sysDescr object in RFC 3418, which includes the full name and version identification of the system's hardware type, software operating system, and networking software.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-description
Console(config-if)#
```

lldp basic-tlv system-name

This command configures an LLDP-enabled port to advertise the system name. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp basic-tlv system-name**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The system name is taken from the sysName object in RFC 3418, which contains the system’s administratively assigned name, and is in turn based on the **hostname** command (page 23-1).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp basic-tlv system-name
Console(config-if)#
```

lldp dot1-tlv proto-ident

This command configures an LLDP-enabled port to advertise the supported protocols. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv proto-ident**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the protocols that are accessible through this interface.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-ident
Console(config-if)#
```

lldp dot1-tlv proto-vid

This command configures an LLDP-enabled port to advertise port related VLAN information. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv proto-vid**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the port-based and protocol-based VLANs configured on this interface (see “Configuring VLAN Interfaces” on page 34-7 and “Configuring Protocol-based VLANs” on page 34-20).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv proto-vid
Console(config-if)#
```

lldp dot1-tlv pvid

This command configures an LLDP-enabled port to advertise its default VLAN ID. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv pvid**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

The port’s default VLAN identifier (PVID) indicates the VLAN with which untagged or priority-tagged frames are associated (see “switchport native vlan” on page 34-10).

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv pvid
Console(config-if)#
```

lldp dot1-tlv vlan-name

This command configures an LLDP-enabled port to advertise its VLAN name. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot1-tlv vlan-name**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises the name of all VLANs to which this interface has been assigned. See “switchport allowed vlan” on page 34-11 and “protocol-vlan protocol-group (Configuring Interfaces)” on page 34-21.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot1-tlv vlan-name
Console(config-if)#
```

lldp dot3-tlv link-agg

This command configures an LLDP-enabled port to advertise link aggregation capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv link-agg**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises link aggregation capabilities, aggregation status of the link, and the 802.3 aggregated port identifier if this interface is currently a link aggregation member.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv link-agg
Console(config-if)#
```

lldp dot3-tlv mac-phy

This command configures an LLDP-enabled port to advertise its MAC and physical layer capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv mac-phy**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises MAC/PHY configuration/status which includes information about auto-negotiation support/capabilities, and operational Multistation Access Unit (MAU) type.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#no lldp dot3-tlv mac-phy
Console(config-if)#
```

lldp dot3-tlv max-frame

This command configures an LLDP-enabled port to advertise its maximum frame size. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv max-frame**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

Refer to “Frame Size Commands” on page 23-9 for information on configuring the maximum frame size for this switch.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv max-frame
Console(config-if)#
```

lldp dot3-tlv poe

This command configures an LLDP-enabled port to advertise its Power-over-Ethernet (PoE) capabilities. Use the **no** form to disable this feature.

Syntax

[**no**] **lldp dot3-tlv poe**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

This option advertises Power-over-Ethernet capabilities, including whether or not PoE is supported, currently enabled, if the port pins through which power is delivered can be controlled, the port pins selected to deliver power, and the power class.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#lldp dot3-tlv poe
Console(config-if)#
```

show lldp config

This command shows LLDP configuration settings for all ports.

Syntax

show lldp config [**detail** *interface*]

- **detail** - Shows configuration summary.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show lldp config

LLDP Global Configuation

 LLDP Enable                : Yes
 LLDP Transmit interval     : 30
 LLDP Hold Time Multiplier  : 4
 LLDP Delay Interval        : 2
 LLDP Reinit Delay          : 2
 LLDP Notification Interval : 5


LLDP Port Configuration
  Interface |AdminStatus NotificationEnabled
  --------- + ----------- -------------------
  Eth 1/1   | Tx-Rx       True
  Eth 1/2   | Tx-Rx       True
  Eth 1/3   | Tx-Rx       True
  Eth 1/4   | Tx-Rx       True
  Eth 1/5   | Tx-Rx       True
⋮
```

```
Console#show lldp config detail ethernet 1/1

LLDP Port Configuration Detail

 Port : Eth 1/1
 Admin Status : Tx-Rx
 Notification Enabled : True
 Basic TLVs Advertised:
   port-description
   system-name
   system-description
   system-capabilities
   management-ip-address
 802.1 specific TLVs Advertised:
  *port-vid
  *vlan-name
  *proto-vlan
  *proto-ident
 802.3 specific TLVs Advertised:
  *mac-phy
  *poe
  *link-agg
  *max-frame

Console#
```

show lldp info local-device

This command shows LLDP global and interface-specific configuration settings for this device.

Syntax

show lldp info local-device [**detail** *interface*]

- **detail** - Shows detailed information.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show lldp info local-device

 LLDP Local System Information
  Chassis Type : MAC Address
  Chassis ID     : 00-01-02-03-04-05
  System Name   :
  System Description : 24/48 port 10/100/1000 Stackable Managed Switch with
                       2 X 10G uplinks
  System Capabilities Support : Bridge, Router
  System Capabilities Enable  : Bridge, Router
  Management Address : 192.168.0.2 (IPv4)

 LLDP Port Information
 Interface |PortID Type       PortID              PortDesc
 --------- + ---------------- ---------------- --------------------------
 Eth 1/1 |MAC Address    00-01-02-03-04-06 Ethernet Port on unit 1, port 1
 Eth 1/2 |MAC Address    00-01-02-03-04-07 Ethernet Port on unit 1, port 2
 Eth 1/3 |MAC Address    00-01-02-03-04-08 Ethernet Port on unit 1, port 3
 Eth 1/4 |MAC Address    00-01-02-03-04-09 Ethernet Port on unit 1, port 4
:
Console#show lldp info local-device detail ethernet 1/1

LLDP Port Information Detail

 Port       : Eth 1/1
 Port Type : MAC Address
 Port ID     : 00-01-02-03-04-06
 Port Desc : Ethernet Port on unit 1, port 1

Console#
```

show lldp info remote-device

This command shows LLDP global and interface-specific configuration settings for remote devices attached to an LLDP-enabled port.

Syntax

show lldp info remote-device [**detail** *interface*]

- **detail** - Shows detailed information.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show lldp info remote-device

 LLDP Remote Devices Information

  Interface | ChassisId          PortId             SysName
  --------- + ----------------- ----------------- ---------------------
  Eth 1/1   | 00-01-02-03-04-05 00-01-02-03-04-06

Console#show lldp info remote-device detail ethernet 1/1

  Chassis Type          : MAC Address
  Chassis Id            : 00-00-E8-90-00-00
  PortID Type           : MAC Address
  PortID                : 00-00-E8-90-00-01
  SysName              :
  SysDescr                   : 24/48 port 10/100/1000 Stackable Managed Switch
                        with 2 X 10G uplinks
  PortDescr              : Ethernet Port on unit 1, port 1
  SystemCapSupported : Bridge, Router
  SystemCapEnabled      : Bridge, Router
  Remote Management Address :
    192.168.0.5 (IPv4)
  Remote Port VID : 1
  Remote Port-Protocol VLAN :
    VLAN-1 : supported, disabled
  Remote VLAN Name :
    VLAN-1 : DefaultVlan
  Remote Protocol Identity (Hex) : 88-CC
  Remote MAC/PHY configuration status :
    Remote port auto-neg supported : Yes
    Remote port auto-neg enabled : Yes
    Remote port auto-neg advertised cap (Hex) : 6C01
    Remote port MAU type : 30

  Remote Link Aggregation :
    Remote link aggregation capable : Yes
    Remote link aggragation enable : No
  Remote link aggragation port id : 0
  Remote Max Frame Size : 1522

Console#
```

show lldp info statistics

This command shows statistics based on traffic received through all attached LLDP-enabled interfaces.

Syntax

show lldp info statistics [**detail** *interface*]

- **detail** - Shows detailed information.
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
switch#show lldp info statistics

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2450279 seconds
  New Neighbor Entries Count         : 1
  Neighbor Entries Deleted Count     : 0
  Neighbor Entries Dropped Count     : 0
  Neighbor Entries Ageout Count      : 0

  Port  | NumFramesRecvd NumFramesSent NumFramesDiscarded
  ----- + -------------- ------------- ------------------
  1     | 0              20            0
  2     | 13             13            0
  3     | 2              2             0
  4     | 0              0             0
  5     | 0              0             0
:
switch#show lldp info statistics detail ethernet 1/1

 LLDP Port Statistics Detail

  PortName          : Eth 1/1
  Frames Discarded  : 0
  Frames Invalid    : 0
  Frames Received   : 12
  Frames Sent       : 13
  TLVs Unrecognized : 0
  TLVs Discarded    : 0
  Neighbor Ageouts  : 0

switch#
```

Chapter 33: Spanning Tree Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the switch, and commands that configure STA for the selected interface.

Table 33-1 Spanning Tree Commands

Command	Function	Mode	Page
spanning-tree	Enables the spanning tree protocol	GC	33-2
spanning-tree mode	Configures STP, RSTP or MSTP mode	GC	33-2
spanning-tree forward-time	Configures the spanning tree bridge forward time	GC	33-4
spanning-tree hello-time	Configures the spanning tree bridge hello time	GC	33-4
spanning-tree max-age	Configures the spanning tree bridge maximum age	GC	33-5
spanning-tree priority	Configures the spanning tree bridge priority	GC	33-6
spanning-tree path-cost method	Configures the path cost method for RSTP/MSTP	GC	33-6
spanning-tree transmission-limit	Configures the transmission limit for RSTP/MSTP	GC	33-7
spanning-tree mst-configuration	Changes to MSTP configuration mode	GC	33-7
mst vlan	Adds VLANs to a spanning tree instance	MST	33-8
mst priority	Configures the priority of a spanning tree instance	MST	33-9
name	Configures the name for the multiple spanning tree	MST	33-9
revision	Configures the revision number for the multiple spanning tree	MST	33-10
max-hops	Configures the maximum number of hops allowed in the region before a BPDU is discarded	MST	33-11
spanning-tree spanning-disabled	Disables spanning tree for an interface	IC	33-11
spanning-tree cost	Configures the spanning tree path cost of an interface	IC	33-12
spanning-tree port-priority	Configures the spanning tree priority of an interface	IC	33-13
spanning-tree edge-port	Enables fast forwarding for edge ports	IC	33-13
spanning-tree portfast	Sets an interface to fast forwarding	IC	33-14
spanning-tree link-type	Configures the link type for RSTP/MSTP	IC	33-15
spanning-tree mst cost	Configures the path cost of an instance in the MST	IC	33-16
spanning-tree mst port-priority	Configures the priority of an instance in the MST	IC	33-17
spanning-tree protocol-migration	Re-checks the appropriate BPDU format	PE	33-17

Table 33-1 Spanning Tree Commands (Continued)

Command	Function	Mode	Page
show spanning-tree	Shows spanning tree configuration for the common spanning tree (i.e., overall bridge), a selected interface, or an instance within the multiple spanning tree	PE	33-18
show spanning-tree mst configuration	Shows the multiple spanning tree configuration	PE	33-20

spanning-tree

This command enables the Spanning Tree Algorithm globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **spanning-tree**

Default Setting

Spanning tree is enabled.

Command Mode

Global Configuration

Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

Example

This example shows how to enable the Spanning Tree Algorithm for the switch:

```
Console(config)#spanning-tree
Console(config)#
```

spanning-tree mode

This command selects the spanning tree mode for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree mode {**stp** | **rstp** | **mstp**}
no spanning-tree mode

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)
- **mstp** - Multiple Spanning Tree (IEEE 802.1s)

Default Setting

rstp

Command Mode

Global Configuration

Command Usage

- Spanning Tree Protocol

  Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.

  - This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

- Rapid Spanning Tree Protocol

  RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

  - STP Mode – If the switch receives an 802.1D BPDU after a port’s migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
  - RSTP Mode – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- Multiple Spanning Tree Protocol

  - To allow multiple spanning trees to operate over the network, you must configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
  - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
  - Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Example

The following example configures the switch to use Rapid Spanning Tree:

```
Console(config)#spanning-tree mode rstp
Console(config)#
```

spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree forward-time *seconds*
no spanning-tree **forward-time**

seconds - Time in seconds. (Range: 4 - 30 seconds)
The minimum value is the higher of 4 or [(max-age / 2) + 1].

Default Setting

15 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree hello-time *time*
no spanning-tree hello-time

time - Time in seconds. (Range: 1-10 seconds).
The maximum value is the lower of 10 or [(max-age / 2) -1].

Default Setting

2 seconds

Command Mode

Global Configuration

Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

Related Commands

spanning-tree forward-time (33-4)
spanning-tree max-age (33-5)

spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree max-age *seconds*
no spanning-tree max-age

seconds - Time in seconds. (Range: 6-40 seconds)
The minimum value is the higher of 6 or [2 x (hello-time + 1)].
The maximum value is the lower of 40 or [2 x (forward-time - 1)].

Default Setting

20 seconds

Command Mode

Global Configuration

Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

Related Commands

spanning-tree forward-time (33-4)
spanning-tree hello-time (33-4)

spanning-tree priority

This command configures the spanning tree priority globally for this switch. Use the **no** form to restore the default.

Syntax

spanning-tree priority *priority*
no spanning-tree priority

priority - Priority of the bridge. (Range: 0 - 65535)
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

Global Configuration

Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (i.e., lower numeric value) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

Example

```
Console(config)#spanning-tree priority 40000
Console(config)#
```

spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree pathcost method {**long** | **short**}
no spanning-tree pathcost method

- **long** - Specifies 32-bit based values that range from 1-200,000,000. This method is based on the IEEE 802.1w Rapid Spanning Tree Protocol.
- **short** - Specifies 16-bit based values that range from 1-65535. This method is based on the IEEE 802.1 Spanning Tree Protocol.

Default Setting

Long method

Command Mode

Global Configuration

Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Note that path cost (page 33-12) takes precedence over port priority (page 33-13).

Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

Syntax

spanning-tree transmission-limit *count*
no spanning-tree transmission-limit

count - The transmission limit in seconds. (Range: 1-10)

Default Setting

3

Command Mode

Global Configuration

Command Usage

This command limits the maximum transmission rate for BPDUs.

Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

spanning-tree mst-configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

Default Setting

- No VLANs are mapped to any MST instance.
- The region name is set the switch’s MAC address.

Command Mode

Global Configuration

Example

```
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#
```

Related Commands

mst vlan (33-8)
mst priority (33-9)
name (33-9)
revision (33-10)
max-hops (33-11)

mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

Syntax

[**no**] **mst** *instance_id* **vlan** *vlan-range*

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *vlan-range* - Range of VLANs. (Range: 1-4093)

Default Setting

none

Command Mode

MST Configuration

Command Usage

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. This switch supports up to 58 instances. You should try to group VLANs which cover the same general area of your network. However, remember that you must configure all bridges within the same MSTI Region (page 33-9) with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

Syntax

mst *instance_id* **priority** *priority*
no mst *instance_id* **priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *priority* - Priority of the a spanning tree instance.
  (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

Default Setting

32768

Command Mode

MST Configuration

Command Usage

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (i.e., lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- You can set this switch to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

Example

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

name

This command configures the name for the multiple spanning tree region in which this switch is located. Use the **no** form to clear the name.

Syntax

name *name*

name - Name of the spanning tree.

Default Setting

Switch’s MAC address

Command Mode

MST Configuration

Command Usage

The MST region name and revision number (page 33-10) are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

Related Commands

revision (33-10)

revision

This command configures the revision number for this multiple spanning tree configuration of this switch. Use the **no** form to restore the default.

Syntax

revision *number*

number - Revision number of the spanning tree. (Range: 0-65535)

Default Setting

0

Command Mode

MST Configuration

Command Usage

The MST region name (page 33-9) and revision number are used to designate a unique MST region. A bridge (i.e., spanning-tree compliant device such as this switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

Related Commands

name (33-9)

max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

Syntax

max-hops *hop-number*

hop-number - Maximum hop number for multiple spanning tree. (Range: 1-40)

Default Setting

20

Command Mode

MST Configuration

Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

Syntax

[**no**] **spanning-tree spanning-disabled**

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree cost *cost*
no spanning-tree cost

cost - The path cost for the port.
(Range: 0 for auto-configuration, 1-65535 for short path cost method[28], 1-200,000,000 for long path cost method)

Table 33-2 Recommended STA Path Cost Range

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Gigabit Ethernet	2,000-65,535	2,000-200,000
10G Ethernet	200-20,000	200-20,000

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021D-2004 standard exceeds 65,535, the default is set to 65,535.

Table 33-3 Default STA Path Costs

Port Type	Short Path Cost (IEEE 802.1D-1998)	Long Path Cost (802.1D-2004)
Gigabit Ethernet	10,000	10,000
10G Ethernet	1,000	1,000

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Path cost takes precedence over port priority.
- When the spanning-tree pathcost method (page 33-6) is set to short, the maximum value for path cost is 65,535.

[28] Use the spanning-tree pathcost method command on page 33-6 to set the path cost method.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

Syntax

spanning-tree port-priority *priority*
no spanning-tree port-priority

priority - The priority for a port. (Range: 0-240, in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on a switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
```

Related Commands

spanning-tree cost (33-12)

spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

Syntax

[**no**] **spanning-tree edge-port**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as the **spanning-tree portfast**.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

Related Commands

spanning-tree portfast (33-14)

spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

Syntax

[**no**] **spanning-tree portfast**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command is used to enable/disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)

- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed for future software versions.

Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#bridge-group 1 portfast
Console(config-if)#
```

Related Commands

spanning-tree edge-port (33-13)

spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree link-type {**auto** | **point-to-point** | **shared**}
no spanning-tree link-type

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

Default Setting

auto

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If you designate a port as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default auto-configuration mode.

Syntax

spanning-tree mst *instance_id* **cost** *cost*
no spanning-tree mst *instance_id* **cost**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)
- *cost* - Path cost for an interface. (Range: 0 for auto-configuration, 1-65535 for short path cost method[29], 1-200,000,000 for long path cost method)

The recommended path cost range is listed in Table 33-2 on page 33-12.

Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode. When the short path cost method is selected and the default path cost recommended by the IEEE 8021D-2004 standard exceeds 65,535, the default is set to 65,535. The default path costs are listed in Table 33-3 on page 33-12.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

Related Commands

spanning-tree mst port-priority (33-17)

[29] Use the spanning-tree pathcost method command on page 33-6 to set the path cost method.

spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

Syntax

spanning-tree mst *instance_id* **port-priority** *priority*
no spanning-tree mst *instance_id* **port-priority**

- *instance_id* - Instance identifier of the spanning tree. (Range: 0-4094, no leading zeroes)
- *priority* - Priority for an interface. (Range: 0-240 in steps of 16)

Default Setting

128

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on a switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

Related Commands

spanning-tree mst cost (33-16)

spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

Syntax

spanning-tree protocol-migration *interface*

interface

- **ethernet** *unit/port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Command Usage

If at any time the switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, you can also use the **spanning-tree protocol-migration** command at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (i.e., RSTP or STP-compatible).

Example

```
Console#spanning-tree protocol-migration eth 1/5
Console#
```

show spanning-tree

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

Syntax

show spanning-tree [*interface* | **mst** *instance_id*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)
- *instance_id* - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the switch for the Common Spanning Tree (CST) and for every interface in the tree.
- Use the **show spanning-tree** *interface* command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the **show spanning-tree mst** *instance_id* command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).
- For a description of the items displayed under “Spanning-tree information,” see “Configuring Global Settings” on page 10-6. For a description of the items

displayed for specific interfaces, see “Displaying Interface Settings” on page 10-10.

Example

```
Console#show spanning-tree
Spanning Tree Information
-------------------------------------------------------------------
 Spanning Tree Mode:                    MSTP
 Spanning Tree Enabled/Disabled:        Enabled
 Instance:                              0
 VLANs Configuration:                   1-4093
 Priority:                              32768
 Bridge Hello Time (sec.):              2
 Bridge Max Age (sec.):                 20
 Bridge Forward Delay (sec.):           15
 Root Hello Time (sec.):                2
 Root Max Age (sec.):                   20
 Root Forward Delay (sec.):             15
 Max  Hops:                             20
 Remaining Hops:                        20
 Designated Root:                        32768.0.0000E8900000
 Current Root Port:                     2
 Current Root Cost:                     10000
 Number of Topology Changes:            2
 Last Topology Change Time (sec.): 4100
 Transmission Limit:                    3
 Path Cost Method:                      Long
-------------------------------------------------------------------
Eth   1/ 1 information
-------------------------------------------------------------------
 Admin Status:                 Enabled
 Role:                         root
 State:                        forwarding
 External Admin Path Cost: 0
 Internal Admin Path Cost: 0
 External Oper Path Cost:  10000
 Internal Oper Path Cost:  10000
 Priority:                     128
 Designated Cost:              0
 Designated Port:              128.1
 Designated Root:               32768.0.0000E8900000
 Designated Bridge:             32768.0.0000E8900000
 Fast Forwarding:              Disabled
 Forward Transitions:          1
 Admin Edge Port:              Disabled
 Oper Edge Port:               Disabled
 Admin Link Type:              auto
 Oper Link Type:                Point-to-point
 Spanning   Tree   Status:                 Enabled
.
.
```

show spanning-tree mst configuration

This command shows the configuration of the multiple spanning tree.

Command Mode

Privileged Exec

Example

```
Console#show spanning-tree mst configuration
Mstp Configuration Information
--------------------------------------------------------------
 Configuration Name: R&D
 Revision level:0

 Instance VLANs
--------------------------------------------------------------
     0    1,3-4093
     1    2
Console#
```

Chapter 34: VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

Table 34-1 VLAN Commands

Command Groups	Function	Page
GVRP and Bridge Extension	Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB	34-1
Editing VLAN Groups	Sets up VLAN groups, including name, VID and state	34-5
Configuring VLAN Interfaces	Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP	34-7
Displaying VLAN Information	Displays VLAN groups, status, port members, and MAC addresses	34-12
Configuring 802.1Q Tunneling	Configures 802.1Q Tunneling (QinQ Tunneling)	34-14
Configuring Private VLANs	Configures private VLANs, including uplink and downlink ports	34-18
Configuring Protocol VLANs	Configures protocol-based VLANs based on frame type and protocol	34-20

GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the switch, as well as how to display default configuration settings for the Bridge Extension MIB.

Table 34-2 GVRP and Bridge Extension Commands

Command	Function	Mode	Page
bridge-ext gvrp	Enables GVRP globally for the switch	GC	34-2
show bridge-ext	Shows the global bridge extension configuration	PE	34-2
switchport gvrp	Enables GVRP for an interface	IC	34-3
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	34-12
show gvrp configuration	Displays GVRP configuration for the selected interface	NE, PE	34-3
garp timer	Sets the GARP timer for the selected function	IC	34-4
show garp timer	Shows the GARP timer for the selected function	NE, PE	34-5

bridge-ext gvrp

This command enables GVRP globally for the switch. Use the **no** form to disable it.

Syntax

[**no**] **bridge-ext gvrp**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

Example

```
Console(config)#bridge-ext gvrp
Console(config)#
```

show bridge-ext

This command shows the configuration for bridge extension commands.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

See “Displaying Basic VLAN Information” on page 11-4 and “Displaying Bridge Extension Capabilities” on page 4-4 for a description of the displayed items.

Example

```
Console#show bridge-ext
 Max support VLAN numbers:              256
 Max support VLAN ID:                   4093
 Extended multicast filtering services: No
 Static entry individual port:          Yes
 VLAN  learning:                        IVL
 Configurable PVID tagging:             Yes
 Local VLAN capable:                    No
 Traffic classes:                        Enabled
 Global GVRP status:                     Disabled
 GMRP:                                   Disabled
Console#
```

switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

Syntax

[**no**] **switchport gvrp**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

show gvrp configuration

This command shows if GVRP is enabled.

Syntax

show gvrp configuration [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows both global and interface-specific configuration.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 GVRP configuration: Disabled
Console#
```

garp timer

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

Syntax

garp timer {**join** | **leave** | **leaveall**} *timer_value*
no garp timer {**join** | **leave** | **leaveall**}

- {**join** | **leave** | **leaveall**} - Which timer to set.
- *timer_value* - Value of timer.
  Ranges:
  join: 20-1000 centiseconds
  leave: 60-3000 centiseconds
  leaveall: 500-18000 centiseconds

Default Setting

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless you are experiencing difficulties with GMRP or GVRP registration/deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.
- Timer values must meet the following restrictions:
  - leave >= (2 x join)
  - leaveall > leave

Note: Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

Related Commands

show garp timer (34-5)

show garp timer

This command shows the GARP timers for the selected interface.

Syntax

show garp timer [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

Shows all GARP timers.

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer:       20 centiseconds
 Leave timer:      60 centiseconds
 Leaveall timer: 1000 centiseconds
Console#
```

Related Commands

garp timer (34-4)

Editing VLAN Groups

Table 34-3 Commands for Editing VLAN Groups

Command	Function	Mode	Page
vlan database	Enters VLAN database mode to add, change, and delete VLANs	GC	34-5
vlan	Configures a VLAN, including VID, name and state	VC	34-6

vlan database

This command enters VLAN database mode. All commands in this mode will take effect immediately.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the VLAN database command mode to add, change, and delete VLANs. After finishing configuration changes, you can display the VLAN settings by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and you can display this file by entering the **show running-config** command.

Example

```
Console(config)#vlan database
Console(config-vlan)#
```

Related Commands

show vlan (34-13)

vlan

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

Syntax

vlan *vlan-id* [**name** *vlan-name*] **media ethernet** [**state** {**active** | **suspend**}]
no vlan *vlan-id* [**name** | **state**]

- *vlan-id* - ID of configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - *vlan-name* - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

Default Setting

By default only VLAN 1 exists and is active.

Command Mode

VLAN Database Configuration

Command Usage

- **no vlan** *vlan-id* deletes the VLAN.
- **no vlan** *vlan-id* **name** removes the VLAN name.
- **no vlan** *vlan-id* **state** returns the VLAN to the default state (i.e., active).
- You can configure up to 4093 VLANs on the switch.

Example

The following example adds a VLAN, using VLAN ID 105 and name RD5. The VLAN is activated by default.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#
```

Related Commands

show vlan (34-13)

Configuring VLAN Interfaces

Table 34-4 Commands for Configuring VLAN Interfaces

Command	Function	Mode	Page
interface vlan	Enters interface configuration mode for a specified VLAN	IC	34-7
switchport mode	Configures VLAN membership mode for an interface	IC	34-8
switchport acceptable-frame-types	Configures frame types to be accepted by an interface	IC	34-9
switchport ingress-filtering	Enables ingress filtering on an interface	IC	34-9
switchport native vlan	Configures the PVID (native VLAN) of an interface	IC	34-10
switchport allowed vlan	Configures the VLANs associated with an interface	IC	34-11
switchport gvrp	Enables GVRP for an interface	IC	34-3
switchport forbidden vlan	Configures forbidden VLANs for an interface	IC	34-12
switchport priority default	Sets a port priority for incoming untagged frames	IC	35-3

interface vlan

This command enters interface configuration mode for VLANs, which is used to configure VLAN parameters for a physical interface.

Syntax

interface vlan *vlan-id*

vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)

Default Setting

None

Command Mode

Global Configuration

Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

Related Commands

shutdown (27-7)

switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

Syntax

switchport mode {**hybrid | trunk**}
no switchport mode

- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (i.e., associated with the PVID) are also transmitted as tagged frames.

Default Setting

All ports are in hybrid mode with the PVID set to VLAN 1.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

Related Commands

switchport acceptable-frame-types (34-9)

switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

Syntax

switchport acceptable-frame-types {**all** | **tagged**}
no switchport acceptable-frame-types

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only receives tagged frames.

Default Setting

All frame types

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

Example

The following example shows how to restrict the traffic received on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

Related Commands

switchport mode (34-8)

switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

Syntax

[**no**] **switchport ingress-filtering**

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Ingress filtering only affects tagged frames.

- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

switchport native vlan

This command configures the PVID (i.e., default VLAN ID) for a port. Use the **no** form to restore the default.

Syntax

switchport native vlan *vlan-id*
no switchport native vlan

vlan-id - Default VLAN ID for a port. (Range: 1-4093, no leading zeroes)

Default Setting

VLAN 1

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- If an interface is not a member of VLAN 1 and you assign its PVID to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before you can assign its PVID to that group.
- If acceptable frame types is set to **all** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

Syntax

switchport allowed vlan {**add** *vlan-list* [**tagged** | **untagged**] |
remove *vlan-list*}
no switchport allowed vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

- All ports are assigned to VLAN 1 by default.
- The default frame type is untagged.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (i.e., 1Q Trunk), then you can only assign an interface to VLAN groups as a tagged member.
- Frames are always tagged within the switch. The tagged/untagged parameter used when adding a VLAN to an interface tells the switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```

switchport forbidden vlan

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

Syntax

switchport forbidden vlan {**add** *vlan-list* | **remove** *vlan-list*}
no switchport forbidden vlan

- **add** *vlan-list* - List of VLAN identifiers to add.
- **remove** *vlan-list* - List of VLAN identifiers to remove.
- *vlan-list* - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4093).

Default Setting

No VLANs are included in the forbidden list.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- This command prevents a VLAN from being automatically added to the specified interface via GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, then you cannot add it to the set of forbidden VLANs for that same interface.

Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

Displaying VLAN Information

This section describes commands used to display VLAN information.

Table 34-5 Commands for Displaying VLAN Information

Command	Function	Mode	Page
show vlan	Shows VLAN information	NE, PE	34-13
show interfaces status vlan	Displays status for the specified VLAN interface	NE, PE	27-9
show interfaces switchport	Displays the administrative and operational status of an interface	NE, PE	27-11

show vlan

This command shows VLAN information.

Syntax

show vlan [**id** *vlan-id* | **name** *vlan-name*]

- **id** - Keyword to be followed by the VLAN ID.
  vlan-id - ID of the configured VLAN. (Range: 1-4093, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  vlan-name - ASCII string from 1 to 32 characters.

Default Setting

Shows all VLANs.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows how to display information for VLAN 1.

```
Console#show vlan id 1

VLAN ID:               1
Type:                  Static
Name:                  DefaultVlan
Status:                Active
Ports/Port Channels:   Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                       Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                       Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                       Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                       Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/25(S)
                       Eth1/26(S)
Console#
```

Configuring IEEE 802.1Q Tunneling

IEEE 802.1Q tunneling (QinQ tunneling) uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

This section describes commands used to configure QinQ tunneling.

Table 34-6 IEEE 802.1Q Tunneling Commands

Command	Function	Mode	Page
dot1q-tunnel system-tunnel-control	Configures the switch to operate in normal mode or QinQ mode	GC	34-15
switchport dot1q-tunnel mode	Configures an interface as a QinQ tunnel port	IC	34-15
switchport dot1q-tunnel tpid	Sets the Tag Protocol Identifier (TPID) value of a tunnel port	IC	34-16
show dot1q-tunnel	Displays the configuration of QinQ tunnel ports	PE	34-17
show interfaces switchport	Displays port QinQ operational status	PE	27-11

General Configuration Guidelines for QinQ

1. Configure the switch to QinQ mode (**dot1q-tunnel system-tunnel-control**, page 34-15).
2. Create a SPVLAN (**vlan**, page 34-6).
3. Configure the QinQ tunnel access port to dot1Q-tunnel access mode (**switchport dot1q-tunnel mode**, page 34-15).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel access port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See **switchport dot1q-tunnel tpid**, page 34-16.)
5. Configure the QinQ tunnel access port to join the SPVLAN as an untagged member (**switchport allowed vlan**, page 34-11).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel access port (**switchport native vlan**, page 34-10).
7. Configure the QinQ tunnel uplink port to dot1Q-tunnel uplink mode (**switchport dot1q-tunnel mode**, page 34-15).
8. Configure the QinQ tunnel uplink port to join the SPVLAN as a tagged member (**switchport allowed vlan**, page 34-11).

Limitations for QinQ

- The native VLAN for the tunnel uplink ports and tunnel access ports cannot be the same. However, the same service VLANs can be set on both tunnel port types.
- IGMP Snooping should not be enabled on a tunnel access port.
- If the spanning tree protocol is enabled, be aware that a tunnel access or tunnel uplink port may be disabled if the spanning tree structure is automatically reconfigured to overcome a break in the tree. It is therefore advisable to disable spanning tree on these ports.

dot1q-tunnel system-tunnel-control

This command sets the switch to operate in QinQ mode. Use the **no** form to disable QinQ operating mode.

Syntax

[**no**] **dot1q-tunnel system-tunnel-control**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

QinQ tunnel mode must be enabled on the switch for QinQ interface settings to be functional.

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#
```

Related Commands

show dot1q-tunnel (34-17)
show interfaces switchport (27-11)

switchport dot1q-tunnel mode

This command configures an interface as a QinQ tunnel port. Use the **no** form to disable QinQ on the interface.

Syntax

switchport dot1q-tunnel mode {**access** | **uplink**}
no switchport dot1q-tunnel mode

- **access** – Sets the port as an 802.1Q tunnel access port.
- **uplink** – Sets the port as an 802.1Q tunnel uplink port.

Default Setting

Disabled

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- QinQ tunneling must be enabled on the switch using the **dot1q-tunnel system-tunnel-control** command before the **switchport dot1q-tunnel mode** interface command can take effect.
- When a tunnel uplink port receives a packet from a customer, the customer tag (regardless of whether there are one or more tag layers) is retained in the inner tag, and the service provider’s tag added to the outer tag.
- When a tunnel uplink port receives a packet from the service provider, the outer service provider’s tag is stripped off, and the packet passed on to the VLAN indicated by the inner tag. If no inner tag is found, the packet is passed onto the native VLAN defined for the uplink port.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#
```

Related Commands

show dot1q-tunnel (34-17)
show interfaces switchport (27-11)

switchport dot1q-tunnel tpid

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the **no** form to restore the default setting.

Syntax

switchport dot1q-tunnel tpid *tpid*
no switchport dot1q-tunnel tpid

tpid – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0800-FFFF hexadecimal)

Default Setting

0x8100

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Use the **switchport dot1q-tunnel tpid** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- All ports on the switch will be set to the same ethertype.

Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel tpid 9100
Console(config-if)#
```

Related Commands

show interfaces switchport (27-11)

show dot1q-tunnel

This command displays information about QinQ tunnel ports.

Command Mode

Privileged Exec

Example

```
Console(config)#dot1q-tunnel system-tunnel-control
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-tunnel mode access
Console(config-if)#interface ethernet 1/2
Console(config-if)#switchport dot1q-tunnel mode uplink
Console(config-if)#end
Console#show dot1q-tunnel

Current double-tagged status of the system is Enabled
The dot1q-tunnel mode of the set interface 1/1 is Access mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/2 is Uplink mode, TPID is 0x8100.
The dot1q-tunnel mode of the set interface 1/3 is Normal mode, TPID is 0x8100.
⋮
```

Related Commands

switchport dot1q-tunnel mode (34-15)

Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. This section describes commands used to configure private VlANs.

Table 34-7 Private VLAN Commands

Command	Function	Mode	Page
pvlan	Enables and configured private VLANS	GC	34-18
show pvlan	Displays the configured private VLANS	PE	34-19

pvlan

This command enables or configures a private VLAN. Use the **no** form to disable the private VLAN.

Syntax

pvlan [**up-link** *interface-list* **down-link** *interface-list*]
no pvlan

- **up-link** – Specifies an uplink interface.
- **down-link** – Specifies a downlink interface.

Default Setting

No private VLANs are defined.

Command Mode

Global Configuration

Command Usage

- A private VLAN provides port-based security and isolation between ports within the VLAN. Data traffic on the downlink ports can only be forwarded to, and from, the uplink port. Data cannot pass between downlink ports in the same private VLAN, nor to ports which do not belong to a private VLAN.
- Any port can be defined as an uplink port or downlink port, but cannot configured to serve both roles.
- Private VLANs and normal VLANs can exist simultaneously within the same switch. Traffic may pass freely between uplink ports in private VLANs and ports in normal VLANs.
- Enter the **pvlan** command without any parameters to enable the private VLAN functions. Then set the interface members for the private VLAN.
- Enter **no pvlan** to disable private VLAN functions and clear the configuration settings for the PVLAN.

Example

This example enables the private VLAN, and then sets port 12 as the uplink and ports 5-8 as the downlinks.

```
Console(config)#pvlan
Console(config)#pvlan up-link ethernet 1/12 down-link ethernet 1/5-8
Console(config)#
```

show pvlan

This command displays the configured private VLAN.

Command Mode

Privileged Exec

Example

```
Console#show pvlan
Private VLAN status: Enabled
Up-link port:
 Ethernet 1/12
Down-link port:
 Ethernet 1/5
 Ethernet 1/6
 Ethernet 1/7
 Ethernet 1/8
Console#
```

Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, you can configure this switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 34-8 Protocol-based VLAN Commands

Command	Function	Mode	Page
protocol-vlan protocol-group	Create a protocol group, specifying the supported protocols	GC	34-20
protocol-vlan protocol-group	Maps a protocol group to a VLAN	IC	34-21
show protocol-vlan protocol-group	Shows the configuration of protocol groups	PE	34-22
show interfaces protocol-vlan protocol-group	Shows the interfaces mapped to a protocol group and the corresponding VLAN	PE	34-22

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the protocols you want to use (page 34-6). Although not mandatory, we suggest configuring a separate VLAN for each major protocol running on your network. Do not add port members at this time.
2. Create a protocol group for each of the protocols you want to assign to a VLAN using the **protocol-vlan protocol-group** command (General Configuration mode).
3. Then map the protocol for each interface to the appropriate VLAN using the **protocol-vlan protocol-group** command (Interface Configuration mode).

protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

Syntax

protocol-vlan protocol-group *group-id* [{**add** | **remove**} **frame-type** *frame* **protocol-type** *protocol*]

no protocol-vlan protocol-group *group-id*

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *frame*[30] - Frame type used by this protocol. (Options: ethernet, rfc-1042, llc-other)

[30] SNAP frame types are not supported by this switch due to hardware limitations.

- *protocol* - Protocol type. The only option for the llc-other frame type is ipx_raw. The options for all other frames types include: ip, ipv6, arp, rarp, and user-defined (0801-FFFF hexadecimal).

Default Setting

No protocol groups are configured.

Command Mode

Global Configuration

Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
 protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type ethernet
 protocol-type arp
Console(config)#
```

protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

Syntax

protocol-vlan protocol-group *group-id* **vlan** *vlan-id*
no protocol-vlan protocol-group *group-id* **vlan**

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *vlan-id* - VLAN to which matching protocol traffic is forwarded. (Range: 1-4093)

Default Setting

No protocol groups are mapped for any interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- When creating a protocol-based VLAN, only assign interfaces via this command. If you assign interfaces using any of the other VLAN commands (such as **vlan** on page 34-6), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.

- If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

Syntax

show protocol-vlan protocol-group [*group-id*]

group-id - Group identifier for a protocol group. (Range: 1-2147483647)

Default Setting

All protocol groups are displayed.

Command Mode

Privileged Exec

Example

This shows protocol group 1 configured for IP over Ethernet:

```
Console#show protocol-vlan protocol-group

 ProtocolGroup ID   Frame Type     Protocol Type
------------------ ------------- ---------------
                 1      ethernet     08 00
Console#
```

show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

Syntax

show interfaces protocol-vlan protocol-group [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Default Setting

The mapping for all interfaces is displayed.

Command Mode

Privileged Exec

Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```
Console#show interfaces protocol-vlan protocol-group

   Port       ProtocolGroup ID     Vlan ID
---------- ------------------ -----------
   Eth 1/1                  1        vlan2
Console#
```

Chapter 35: Class of Service Commands

The commands described in this section allow you to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the relative weight of each queue, and the mapping of frame priority tags to the switch's priority queues.

Table 35-1 Priority Commands

Command Groups	Function	Page
Priority (Layer 2)	Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues	35-1
Priority (Layer 3 and 4)	Sets the default priority processing method (CoS, IP Precedence or DSCP); and maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values	35-7

Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the switch.

Table 35-2 Priority Commands (Layer 2)

Command	Function	Mode	Page
queue mode	Sets the queue mode to strict priority or Weighted Round-Robin (WRR)	GC	35-2
switchport priority default	Sets a port priority for incoming untagged frames	IC	35-3
queue bandwidth	Assigns round-robin weights to the priority queues	IC	35-4
queue cos-map	Assigns class-of-service values to the priority queues	IC	35-4
show queue mode	Shows the current queue mode	PE	35-5
show queue bandwidth	Shows round-robin weights assigned to the priority queues	PE	35-6
show queue cos-map	Shows the class-of-service map	PE	35-6
show interfaces switchport	Displays the administrative and operational status of an interface	PE	27-11

queue mode

This command sets the queue mode to strict priority or Weighted Round-Robin (WRR) for the class of service (CoS) priority queues. Use the **no** form to restore the default value.

Syntax

queue mode {**strict** | **wrr**}
no queue mode

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 - 7 respectively.

Default Setting

Weighted Round Robin

Command Mode

Global Configuration

Command Usage

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, or use Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.

Example

The following example sets the queue mode to strict priority service mode:

```
Console(config)#queue mode strict
Console(config)#
```

Related Commands

queue bandwidth (35-4)
show queue mode (35-5)

switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

Syntax

switchport priority default *default-priority-id*
no switchport priority default

default-priority-id - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- This switch provides eight priority queues for each port. It is configured to use strict priority queuing or Weighted Round Robin using the **queue mode** command (see page 35-2). Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 2 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport priority default 5
```

Related Commands

show interfaces switchport (27-11)

queue bandwidth

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues. Use the **no** form to restore the default weights.

Syntax

queue bandwidth *weight0...weight7*
no queue bandwidth

weight0...weight7 - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1 - 15)

Default Setting

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- WRR controls bandwidth sharing at the egress port by defining scheduling weights.
- Bandwidth is allocated to each queue by calculating a precise number of bytes per second that will be serviced on each round. The granularity used to calculate this number is based on a unit of 2k bytes. The bytes serviced per second per queue in each round is (queue weight*granularity).

Example

This example shows how to assign WRR weights to each of the priority queues:

```
Console#configure
Console(config)#int eth 1/5
Console(config-if)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config-if)#
```

Related Commands

show queue bandwidth (35-6)

queue cos-map

This command assigns class of service (CoS) values to the priority queues (i.e., hardware output queues 0 - 7). Use the **no** form set the CoS map to the default values.

Syntax

queue cos-map *queue_id* [*cos1 ... cosn*]
no queue cos-map

- *queue_id* - The ID of the priority queue.
  Ranges are 0 to 7, where 7 is the highest priority queue.

- *cos1 ... cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

Default Setting

This switch supports Class of Service by using eight priority queues, with Weighted Round Robin queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown below.

Table 35-3 Default CoS Priority Levels

Priority	0	1	2	3	4	5	6	7
Queue	2	0	1	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- CoS values assigned at the ingress port are also used at the egress port.
- This command sets the CoS priority for all interfaces.

Example

The following example shows how to change the CoS assignments to a one-to-one mapping:

```
Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#
```

Related Commands

show queue cos-map (35-6)

show queue mode

This command shows the current queue mode.

Command Mode

Privileged Exec

Example

```
Console#show queue mode

Queue Mode: wrr
Console#
```

show queue bandwidth

This command displays the weighted round-robin (WRR) bandwidth allocation for the eight priority queues.

Syntax

show queue bandwidth [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show queue bandwidth
Information of Eth 1/1
 Queue ID   Weight
 --------   ------
    0         1
    1         2
    2         4
    3         6
    4         8
    5         10
    6         12
    7         14
⋮
```

show queue cos-map

This command shows the class of service priority map.

Syntax

show queue cos-map [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value:        0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and Layer 4 traffic priority on the switch.

Table 35-4 Priority Commands (Layer 3 and 4)

Command	Function	Mode	Page
map ip port	Enables TCP/UDP class of service mapping	GC	35-7
map ip port	Maps TCP/UDP socket to a class of service	IC	35-8
map ip precedence	Enables IP precedence class of service mapping	GC	35-8
map ip precedence	Maps IP precedence value to a class of service	IC	35-9
map ip dscp	Enables IP DSCP class of service mapping	GC	35-10
map ip dscp	Maps IP DSCP value to a class of service	IC	35-10
show map ip port	Shows the IP port map	PE	35-11
show map ip precedence	Shows the IP precedence map	PE	35-12
show map ip dscp	Shows the IP DSCP map	PE	35-13

map ip port (Global Configuration)

This command enables IP port mapping (i.e., class of service mapping for TCP/UDP sockets). Use the **no** form to disable IP port mapping.

Syntax

[**no**] **map ip port**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

Example

The following example shows how to enable TCP/UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```

map ip port (Interface Configuration)

This command sets IP port priority (i.e., TCP/UDP port priority). Use the **no** form to remove a specific setting.

Syntax

map ip port *port-number* **cos** *cos-value*
no map ip port *port-number*

- *port-number* - 16-bit TCP/UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

None

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- Up to 8 entries can be specified for IP Port priority mapping.
- This command sets the IP port priority for all interfaces.

Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

map ip precedence (Global Configuration)

This command enables IP precedence mapping (i.e., IP Type of Service). Use the **no** form to disable IP precedence mapping.

Syntax

[**no**] **map ip precedence**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

map ip precedence (Interface Configuration)

This command sets IP precedence priority (i.e., IP Type of Service priority). Use the **no** form to restore the default table.

Syntax

map ip precedence *ip-precedence-value* **cos** *cos-value*
no map ip precedence

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The list below shows the default priority mapping.

Table 35-5 Mapping IP Precedence to CoS Values

IP Precedence Value	0	1	2	3	4	5	6	7
CoS Value	0	1	2	3	4	5	6	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP Precedence for all interfaces.

Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

map ip dscp (Global Configuration)

This command enables IP DSCP mapping (i.e., Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

Syntax

[**no**] **map ip dscp**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

map ip dscp (Interface Configuration)

This command sets IP DSCP priority (i.e., Differentiated Services Code Point priority). Use the **no** form to restore the default table.

Syntax

map ip dscp *dscp-value* **cos** *cos-value*
no map ip dscp

- *dscp-value* - 8-bit DSCP value. (Range: 0-63)
- *cos-value* - Class-of-Service value (Range: 0-7)

Default Setting

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 35-6 Mapping IP DSCP to CoS Values

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

show map ip port

This command shows the IP port priority map.

Syntax

show map ip port [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port      Port no. COS
 --------- -------- ---
  Eth 1/ 5       80   0
Console#
```

Related Commands

map ip port (Global Configuration) (35-7)
map ip port (Interface Configuration) (35-8)

show map ip precedence

This command shows the IP precedence priority map.

Syntax

show map ip precedence [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

 Port      Precedence COS
 --------- ---------- ---
  Eth 1/ 5          0   0
  Eth 1/ 5          1   1
  Eth 1/ 5          2   2
  Eth 1/ 5          3   3
  Eth 1/ 5          4   4
  Eth 1/ 5          5   5
  Eth 1/ 5          6   6
  Eth 1/ 5          7   7
Console#
```

Related Commands

map ip precedence (Global Configuration) (35-8)
map ip precedence (Interface Configuration) (35-9)

show map ip dscp

This command shows the IP DSCP priority map.

Syntax

show map ip dscp [*interface*]

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

 Port       DSCP COS
 --------- ---- ---
  Eth 1/ 1     0   0
  Eth 1/ 1     1   0
  Eth 1/ 1     2   0
  Eth 1/ 1     3   0
⋮
  Eth 1/ 1   61   0
  Eth 1/ 1   62   0
  Eth 1/ 1   63   0
Console#
```

Related Commands

map ip dscp (Global Configuration) (35-10)
map ip dscp (Interface Configuration) (35-10)

Chapter 36: Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. You can classify traffic based on access lists, IP Precedence or DSCP values, or VLANs. Using access lists allows you select traffic based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

Table 36-1 Quality of Service Commands

Command	Function	Mode	Page
class-map	Creates a class map for a type of traffic	GC	36-2
match	Defines the criteria used to classify traffic	CM	36-3
rename	Redefines the name of a class map	CM	36-4
description	Specifies the description of a class map	CM	36-4
policy-map	Creates a policy map for multiple interfaces	GC	36-5
class	Defines a traffic classification for the policy to act on	PM	36-5
rename	Redefines the name of a policy map	PM	36-4
description	Specifies the description of a policy map	PM	36-4
set	Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in a packet	PM-C	36-6
police	Defines an enforcer for classified traffic	PM-C	36-7
service-policy	Applies a policy map defined by the **policy-map** command to the input of a particular interface	IC	36-8
show class-map	Displays the QoS class maps which define matching criteria used for classifying traffic	PE	36-9
show policy-map	Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations	PE	36-9
show policy-map interface	Displays the configuration of a **l** classes configured for a **l** service policies on the specified interface	PE	36-10

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the **class-map** command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the **match** command to select a specific type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Use the **policy-map** command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
4. Use the **class** command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain multiple class statements.
5. Use the **set** command to modify the QoS value for matching traffic class, and use the **policer** command to monitor the average flow and burst rate, and drop

any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.

6. Use the **service-policy** command to assign a policy map to a specific interface.

Notes: **1.** You can configure up to 16 rules per Class Map. You can also include multiple classes in a Policy Map.

2. You should create a Class Map (page 36-2) before creating a Policy Map (page 36-5). Otherwise, you will not be able to specify a Class Map with the **class** command (page 36-5) after entering Policy-Map Configuration mode.

class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map and return to Global configuration mode.

Syntax

[**no**] **class-map** *class-map-name* [**match-any**]

- **match-any** - Match any condition within a class map.
- *class-map-name* - Name of the class map. (Range: 1-16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use the **match** command (page 36-3) to specify the criteria for ingress traffic that will be classified under this class map.
- Up to 16 **match** commands are permitted per class map.
- One or more class maps can be assigned to a policy map (page 36-5). The policy map is then bound by a service policy to an interface (page 36-8). A service policy defines packet classification, service tagging, and bandwidth policing. Once a policy map has been bound to an interface, no additional class maps may be added to the policy map, nor any changes made to the assigned class maps with the **match** or **set** commands.

Example

This example creates a class map call “rd_class,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

Related Commands

show class map (36-9)

match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

Syntax

[**no**] **match** {**access-list** *acl-name* | **ip dscp** *dscp* | **ipv6 dscp** *dscp* | **ip precedence** *ip-precedence* | **vlan** *vlan*}

- *acl-name* - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- *dscp* - A Differentiated Service Code Point value. (Range: 0-63)
- *ip-precedence* - An IP Precedence value. (Range: 0-7)
- *vlan* - A VLAN. (Range:1-4093)

Default Setting

None

Command Mode

Class Map Configuration

Command Usage

- First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use the **match** command to specify the fields within ingress packets that must match to qualify for this class map.
- If an ingress packet matches an ACL specified by this command, any deny rules included in the ACL will be ignored.
- If match criteria includes an IP ACL or IP priority rule, then a VLAN rule cannot be included in the same class map.

  If match criteria includes a MAC ACL or VLAN rule, then neither an IP ACL nor IP priority rule can be included in the same class map.
- Up to 16 **match** commands are permitted per class map.

Example

This example creates a class map called “rd_class#1,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#
```

This example creates a class map call “rd_class#2,” and sets it to match packets marked for IP Precedence service value 5:

```
Console(config)#class-map rd_class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#
```

This example creates a class map call “rd_class#3,” and sets it to match packets marked for VLAN 1.

```
Console(config)#class-map rd_class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#
```

rename

This command redefines the name of a class map or policy map.

Syntax

rename *map-name*

map-name - Name of the class map or policy map. (Range: 1-16 characters)

Command Mode

Class Map Configuration
Policy Map Configuration

Example

```
Console(config)#class-map rd-class#1
Console(config-cmap)#rename rd-class#9
Console(config-cmap)#
```

description

This command specifies the description of a class map or policy map.

Syntax

description *string*

string - Description of the class map or policy map. (Range: 1-64 characters)

Command Mode

Class Map Configuration
Policy Map Configuration

Example

```
Console(config)#class-map rd_class#1
Console(config-cmap)#description matches packets marked for DSCP service
  value 3
Console(config-cmap)#
```

policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map.

Syntax

[**no**] **policy-map** *policy-map-name*

policy-map-name - Name of the policy map. (Range: 1-16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command (page 36-8).
- Create a Class Map (page 36-5) before assigning it to a Policy Map.

Example

This example creates a policy called “rd_policy,” uses the **class** command to specify the previously defined “rd_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map.

Syntax

[**no**] **class** *class-map-name*

class-map-name - Name of the class map. (Range: 1-16 characters)

Default Setting

None

Command Mode

Policy Map Configuration

Command Usage

- Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** and **police** commands to specify the match criteria, where the:
  - **set** command classifies the service that an IP packet will receive.
  - **police** command defines the maximum throughput, burst rate, and the action that results from a policy violation.
- You can configure up to 16 rules per Class Map. You can also include multiple classes in a Policy Map.

Example

This example creates a policy called “rd_policy,” uses the **class** command to specify the previously defined “rd_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

set

This command services IP traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified by the **match** command on page 36-3). Use the **no** form to remove the traffic classification.

Syntax

[**no**] **set** {**cos** *new-cos* | **ip dscp** *new-dscp* | **ip precedence** *new-precedence* | **ipv6 dscp** *new-dscp*}

- *new-cos* - New Class of Service (CoS) value. (Range: 0-7)
- *new-dscp* - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)
- *new-precedence* - New IP Precedence value. (Range: 0-7)

Default Setting

None

Command Mode

Policy Map Class Configuration

Example

This example creates a policy called “rd_policy,” uses the **class** command to specify the previously defined “rd_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

police

This command defines an policer for classified traffic based on the metered flow rate. Use the **no** form to remove a policer.

Syntax

[**no**] **police** *rate-kbps burst-byte* [**exceed-action** {**drop** | **set**}]

- *rate-kbps* - Committed information rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
- *burst-byte* - Committed burst size in bytes. (Range: 64-524288 bytes)
- **drop** - Drop packet when specified rate or burst are exceeded.
- **set** - Set DSCP service to the specified value. (Range: 0-63)

Default Setting

Drop out-of-profile packets.

Command Mode

Policy Map Class Configuration

Command Usage

- You can configure up to 64 policers (i.e., meters or class maps) for each of the following access list types: MAC ACL, IP ACL (including Standard ACL and Extended ACL), IPv6 Standard ACL, and IPv6 Extended ACL. This limitation applies to each switch chip (IC40240-10G: ports 1-26, IC40480-10G: ports 1-25, ports 26-50).
- Policing is based on a token bucket, where bucket depth (i.e., the maximum burst before the bucket overflows) is by specified the *burst-byte* field, and the average rate tokens are removed from the bucket is by specified by the *rate-bps* option.

Example

This example creates a policy called “rd_policy,” uses the **class** command to specify the previously defined “rd_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

service-policy

This command applies a policy map defined by the **policy-map** command to the ingress queue of a particular interface. Use the **no** form to remove the policy map from this interface.

Syntax

[**no**] **service-policy input** *policy-map-name*

- **input** - Apply to the input traffic.
- *policy-map-name* - Name of the policy map for this interface. (Range: 1-16 characters)

Default Setting

No policy map is attached to an interface.

Command Mode

Interface Configuration (Ethernet, Port Channel)

Command Usage

- Only one policy map can be assigned to an interface.
- First define a class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.
- The switch does not allow a policy map to be bound to an interface for egress traffic.

Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

Syntax

show class-map [*class-map-name*]

class-map-name - Name of the class map. (Range: 1-16 characters)

Default Setting

Displays all class maps.

Command Mode

Privileged Exec

Example

```
Console#show class-map
Class Map match-any rd_class#1
 Match ip dscp 3

Class Map match-any rd_class#2
 Match ip precedence 5

Class Map match-any rd_class#3
 Match vlan 1

Console#
```

show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

Syntax

show policy-map [*policy-map-name* [**class** *class-map-name*]]

- *policy-map-name* - Name of the policy map. (Range: 1-16 characters)
- *class-map-name* - Name of the class map. (Range: 1-16 characters)

Default Setting

Displays all policy maps and all classes.

Command Mode

Privileged Exec

Example

```
Console#show policy-map
Policy Map rd_policy
 class rd_class
  set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
 class rd_class
  set ip dscp 3
Console#
```

show policy-map interface

This command displays the service policy assigned to the specified interface.

Syntax

show policy-map interface *interface* **input**

interface

- **ethernet** *unit*/*port*
  - *unit* - Stack unit. (Range: 1-8)
  - *port* - Port number. (Range: 1-26/50)
- **port-channel** *channel-id* (Range: 1-32)

Command Mode

Privileged Exec

Example

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```

Chapter 37: Multicast Filtering Commands

This switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

Table 37-1 Multicast Filtering Commands

Command Groups	Function	Page
IGMP Snooping	Configures multicast groups via IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members	37-1
IGMP Query	Configures IGMP query parameters for multicast filtering at Layer 2	37-5
Static Multicast Interface	Configures static multicast router ports which forward all inbound multicast traffic to the attached VLANs	37-9

IGMP Snooping Commands

This section describes commands used to configure IGMP snooping on the switch.

Table 37-2 IGMP Snooping Commands

Command	Function	Mode	Page
ip igmp snooping	Enables IGMP snooping	GC	37-1
ip igmp snooping vlan static	Adds an interface as a member of a multicast group	GC	37-2
ip igmp snooping version	Configures the IGMP version for snooping	GC	37-2
ip igmp snooping immediate-leave	Immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN	IC	37-3
show ip igmp snooping	Shows the IGMP snooping and query configuration	PE	37-4
show mac-address-table multicast	Shows the IGMP snooping MAC multicast list	PE	37-4

ip igmp snooping

This command enables IGMP snooping on this switch. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping**

Default Setting

Enabled

Command Mode

Global Configuration

Example

The following example enables IGMP snooping.

```
Console(config)#ip igmp snooping
Console(config)#
```

ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **static** *ip-address interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *ip-address* - IP address for multicast group
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Static multicast entries are never aged out.
- When a multicast entry is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet 1/5
Console(config)#
```

ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

Syntax

ip igmp snooping {**1** | **2** | **3**}
no ip igmp snooping version

- **1** - IGMP Version 1
- **2** - IGMP Version 2
- **3** - IGMP Version 3

Default Setting

IGMP Version 2

Command Mode

Global Configuration

Command Usage

- This command configures the IGMP report/query version used by IGMP snooping. Versions 1 - 3 are all supported, and versions 2 and 3 are backward compatible, so the switch can operate with other devices, regardless of the snooping version employed.
- Some commands are only enabled for IGMPv2, including **ip igmp query-max-response-time** and **ip igmp query-timeout**.

Example

The following configures the switch to use IGMP Version 1.

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

ip igmp snooping immediate-leave

This command immediately deletes a member port of a multicast service if a leave packet is received at that port and immediate-leave is enabled for the parent VLAN. Use the **no** form to restore the default.

Syntax

[**no**] **ip igmp snooping immediate-leave**

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- If immediate-leave is *not* used, a multicast router (or querier) will send a group-specific query message when an IGMPv2/v3 group leave message is received. The router/querier stops forwarding traffic for that group only if no host replies to the query within the timeout period (see the **ip igmp snooping query-count** and **ip igmp snooping query-max-response-time** commands on page 37-6 and 37-7).
- If immediate-leave is enabled, the switch assumes that only one host is connected to the interface. Therefore, immediate leave should only be enabled on an interface if it is connected to only one IGMP-enabled device, either a service host or a neighbor running IGMP snooping.
- This command is only effective if IGMP snooping is enabled, and IGMPv2 or IGMPv3 snooping is used.

Example

The following shows how to enable immediate leave.

```
Console(config)#ip igmp snooping vlan 1 immediate-leave
Console(config)#
```

show ip igmp snooping

This command shows the IGMP snooping and query configuration settings.

Command Mode

Privileged Exec

Command Usage

See "Configuring IGMP Snooping and Query Parameters" on page 15-3 for a description of the displayed items.

Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
 Service Status:           Enabled
 Querier Status:           Disabled
 Query Count:             2
 Query Interval:           125 sec
 Query Max Response Time: 10 sec
 Router Port Expire Time: 300 sec
 Immediate Leave Processing: Disabled on all VLAN
 IGMP Snooping Version:    Version 2
Console#
```

show mac-address-table multicast

This command shows known multicast group, source, and host port mappings for the specified interface (or for all interfaces if none is specified), or for a specified multicast address.

Syntax

show mac-address-table multicast [*interface* [**user** | **igmp-snooping**]] [**user** | **igmp-snooping**] [*multicast-address*]

- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)
  - **vlan** *vlan-id* - VLAN ID (1-4093)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.
- *multicast-address* - An IP multicast group address.
  (Range: 224.0.0.0 to 239.255.255.255)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

Member types displayed include IGMP or USER, depending on selected options.

Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
 VLAN M'cast IP addr. Member ports Type
 ---- -------------- ----------- -------
    1        224.1.2.3       Eth1/11     IGMP
Console#
```

IGMP Query Commands

This section describes commands used to configure IGMP query on the switch.

Table 37-3 IGMP Query Commands

Command	Function	Mode	Page
ip igmp snooping querier	Allows this device to act as the querier for IGMP snooping	GC	37-5
ip igmp snooping query-count	Configures the query count	GC	37-6
ip igmp snooping query-interval	Configures the query interval	GC	37-7
ip igmp snooping query-max-response-time	Configures the report delay	GC	37-7
ip igmp snooping router-port-expire-time	Configures the query timeout	GC	37-8

ip igmp snooping querier

This command enables the switch as an IGMP querier. Use the **no** form to disable it.

Syntax

[**no**] **ip igmp snooping querier**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If enabled, the switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

Example

```
Console(config)#ip igmp snooping querier
Console(config)#
```

ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-count *count*
no ip igmp snooping query-count

count - The maximum number of queries issued for which there has been no response before the switch takes action to drop a client from the multicast group. (Range: 2-10)

Default Setting

2 times

Command Mode

Global Configuration

Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

Related Commands

ip igmp snooping query-max-response-time (37-7)

ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-interval *seconds*
no ip igmp snooping query-interval

seconds - The frequency at which the switch sends IGMP host-query messages. (Range: 60-125)

Default Setting

125 seconds

Command Mode

Global Configuration

Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

ip igmp snooping query-max-response-time

This command configures the query report delay. Use the **no** form to restore the default.

Syntax

ip igmp snooping query-max-response-time *seconds*
no ip igmp snooping query-max-response-time

seconds - The report delay advertised in IGMP queries. (Range: 5-25)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

- The switch must be using IGMPv2 for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 20
Console(config)#
```

Related Commands

ip igmp snooping version (37-2)
ip igmp snooping query-max-response-time (37-7)

ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form to restore the default.

Syntax

ip igmp snooping router-port-expire-time *seconds*
no ip igmp snooping router-port-expire-time

seconds - The time the switch waits after the previous querier stops before it considers the router port (i.e., the interface which had been receiving query packets) to have expired. (Range: 300-500)

Default Setting

300 seconds

Command Mode

Global Configuration

Command Usage

The switch must use IGMPv2 for this command to take effect.

Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#
```

Related Commands

ip igmp snooping version (37-2)

Static Multicast Routing Commands

This section describes commands used to configure static multicast interfaces on the switch.

Table 37-4 Static Multicast Routing Commands

Command	Function	Mode	Page
ip igmp snooping vlan mrouter	Adds a multicast router port	GC	37-9
show ip igmp snooping mrouter	Shows multicast router ports	PE	37-10

ip igmp snooping vlan mrouter

This command statically configures a multicast router port on the specified VLAN. Use the **no** form to remove the configuration.

Syntax

[**no**] **ip igmp snooping vlan** *vlan-id* **mrouter** *interface*

- *vlan-id* - VLAN ID (Range: 1-4093)
- *interface*
  - **ethernet** *unit*/*port*
    - *unit* - Stack unit. (Range: 1-8)
    - *port* - Port number. (Range: 1-26/50)
  - **port-channel** *channel-id* (Range: 1-32)

Default Setting

No static multicast router ports are configured.

Command Mode

Global Configuration

Command Usage

Depending on your network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/switch connected over the network to an interface (port or trunk) on your router, you can manually configure that interface to join all the current multicast groups.

Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

Syntax

show ip igmp snooping mrouter [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Default Setting

Displays multicast router ports for all configured VLANs.

Command Mode

Privileged Exec

Command Usage

Multicast router port types displayed include Static.

Example

The following shows that port 11 in VLAN 1 is attached to a multicast router:

```
Console#show ip igmp snooping mrouter vlan 1
 VLAN M'cast Router Ports Type
 ---- ------------------- -------
    1            Eth 1/11   Static
Console#
```

Chapter 38: Domain Name Service Commands

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the **ip name-server** command and domain lookup is enabled with the **ip domain-lookup** command.

Table 38-1 DNS Commands

Command	Function	Mode	Page
ip host	Creates a static host name-to-address mapping	GC	38-1
clear host	Deletes entries from the host name-to-address table	PE	38-2
ip domain-name	Defines a default domain name for incomplete host names	GC	38-3
ip domain-list	Defines a list of default domain names for incomplete host names	GC	38-3
ip name-server	Specifies the address of one or more name servers to use for host name-to-address translation	GC	38-4
ip domain-lookup	Enables DNS-based host name-to-address translation	GC	38-5
show hosts	Displays the static host name-to-address mapping table	PE	38-6
show dns	Displays the configuration for DNS services	PE	38-7
show dns cache	Displays entries in the DNS cache	PE	38-7
clear dns cache	Clears all entries from the DNS cache	PE	38-8

ip host

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the **no** form to remove an entry.

Syntax

[**no**] **ip host** *name address1* [*address2* … *address8*]

- *name* - Name of the host. (Range: 1-127 characters)
- *address1* - Corresponding IP address.
- *address2* … *address8* - Additional corresponding IP addresses.

Default Setting

No static entries

Command Mode

Global Configuration

Command Usage

Servers or other network devices may support one or more connections via multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.

Example

This example maps two address to a host name.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
Console#
```

clear host

This command deletes entries from the DNS table.

Syntax

clear host {*name* | *}

- *name* - Name of the host. (Range: 1-127 characters)
- * - Removes all entries.

Default Setting

None

Command Mode

Privileged Exec

Example

This example clears all static entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

ip domain-name

This command defines the default domain name appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

Syntax

ip domain-name *name*
no ip domain-name

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
Name Server List:
Console#
```

Related Commands

ip domain-list (38-3)
ip name-server (38-4)
ip domain-lookup (38-5)

ip domain-list

This command defines a list of domain names that can be appended to incomplete host names (i.e., host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

Syntax

[**no**] **ip domain-list** *name*

name - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-127 characters; 1-3 names)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on this switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the **ip domain-name** command is used. If there is a domain list, the default domain name is not used.

Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
Console#
```

Related Commands

ip domain-name (38-3)

ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

Syntax

[**no**] **ip name-server** *server-address1* [*server-address2* … *server-address6*]

- *server-address1* - IP address of domain-name server.
- *server-address2* … *server-address6* - IP address of additional domain-name servers.

Default Setting

None

Command Mode

Global Configuration

Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Example

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS disabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

Related Commands

ip domain-name (38-3)
ip domain-lookup (38-5)

ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

Syntax

[**no**] **ip domain-lookup**

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- At least one name server must be specified before you can enable DNS.
- If all name servers are deleted, DNS will automatically be disabled.

Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.jp
    .sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
```

Related Commands

ip domain-name (38-3)
ip name-server (38-4)

show hosts

This command displays the static host name-to-address mapping table.

Command Mode

Privileged Exec

Example

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```

show dns

This command displays the configuration of the DNS service.

Command Mode

Privileged Exec

Example

```
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    sample.com
Domain Name List:
    sample.com.jp
    sample.com.uk
Name Server List:
    192.168.1.55
    10.1.0.55
Console#
```

show dns cache

This command displays entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#show dns cache
NO       FLAG     TYPE     DOMAIN                          TTL      IP
0        4       Address www.times.com                     198      199.239.136.200
1        4       Address a1116.x.akamai.net                19       61.213.189.120
2        4       Address a1116.x.akamai.net                 19       61.213.189.104
3        4       CNAME    graphics8.nytimes.com            19        POINTER TO:2
4        4       CNAME     graphics478.nytimes.com.edgesui 19        POINTER TO:2
Console#
```

Table 38-2   show dns cache - display description

Field	Description
NO	The entry number for each resource record.
FLAG	The flag is always “4” indicating a cache entry and therefore unreliable.
TYPE	This field includes ADDRESS which specifies the host address for the owner, and CNAME which specifies an alias.
IP	The IP address associated with this record.
TTL	The time to live reported by the name server.
DOMAIN	The domain name associated with this record.

clear dns cache

This command clears all entries in the DNS cache.

Command Mode

Privileged Exec

Example

```
Console#clear dns cache
Console#show dns cache
NO      FLAG    TYPE    IP              TTL     DOMAIN
Console#
```

Chapter 39: DHCP Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. You can configure any VLAN interface to be automatically assigned an IP address via DHCP. This switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or you can configure this switch to provide DHCP service directly to any client.

Table 39-1 DHCP Commands

Command Group	Function	Page
DHCP Client	Allows interfaces to dynamically acquire IP address information	39-1
DHCP Relay	Relays DHCP requests from local hosts to a remote DHCP server	39-3
DHCP Server	Configures DHCP service using address pools or static bindings	39-5

DHCP Client

Use the commands in this section to allow the switch's VLAN interfaces to dynamically acquire IP address information.

Table 39-2 DHCP Client Commands

Command	Function	Mode	Page
ip dhcp client-identifier	Specifies the DHCP client identifier for this switch	IC	39-1
ip dhcp restart client	Submits a BOOTP or DHCP client request	PE	39-2

ip dhcp client-identifier

This command specifies the DCHP client identifier for the current interface. Use the **no** form to remove this identifier.

Syntax

ip dhcp client-identifier {**text** *text* | **hex** *hex*}
no ip dhcp client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to include a client identifier in all communications with the DHCP server, which uses it to index its database of address bindings. The information included in the identifier is based on RFC 2132 Option 60, and must be unique for all clients in the same administrative domain.

Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

Related Commands

ip dhcp restart client (39-2)

ip dhcp restart client

This command submits a BOOTP or DHCP client request.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode via the **ip address** command.
- DHCP requires the server to reassign the client’s last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.1.54, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip address (41-3)

DHCP Relay

Table 39-3 DHCP Relay Commands

Command	Function	Mode	Page
ip dhcp restart relay	Enables DHCP relay agent	IC	39-3
ip dhcp relay server	Specifies DHCP server addresses for relay	IC	39-4

ip dhcp restart relay

This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

Syntax

[**no**] **ip dhcp relay**

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

This command is used to configure DHCP relay functions for host devices attached to the switch. If DHCP relay service is enabled, and this switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client’s subnet, and sends a DHCP response back to the DHCP relay agent (i.e., this switch). This switch then broadcasts the DHCP response received from the server to the client.

Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
  Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#
```

Related Commands

ip dhcp relay server (39-4)

ip dhcp relay server

This command specifies the addresses of DHCP servers to be used by the switch’s DHCP relay agent. Use the **no** form to clear all addresses.

Syntax

ip dhcp relay server *address1* [*address2* [*address3 ...*]]
no ip dhcp relay server

address - IP address of DHCP server. (Range: 1-3 addresses)

Default Setting

None

Command Mode

Interface Configuration (VLAN)

Usage Guidelines

- You must specify the IP address for at least one DHCP server. Otherwise, the switch’s DHCP relay agent will not forward client requests to a DHCP server.
- To start DHCP relay service, enter the **ip dhcp restart relay** command.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

Related Commands

ip dhcp restart relay (39-3)

DHCP Server

Table 39-4 DHCP Server Commands

Command	Function	Mode	Page
service dhcp	Enables the DHCP server feature on this switch	GC	39-5
ip dhcp excluded-address	Specifies IP addresses that a DHCP server should not assign to DHCP clients	GC	39-6
ip dhcp pool	Configures a DHCP address pool on a DHCP Server	GC	39-6
network	Configures the subnet number and mask for a DHCP address pool	DC	39-7
default-router	Specifies the default router list for a DHCP client	DC	39-8
domain-name	Specifies the domain name for a DHCP client	DC	39-8
dns-server	Specifies the Domain Name Server (DNS) servers available to a DHCP client	DC	39-9
next-server	Configures the next server in the boot process of a DHCP client	DC	39-9
bootfile	Specifies a default boot image for a DHCP client	DC	39-10
netbios-name-server	Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients	DC	39-10
netbios-node-type	Configures NetBIOS node type for Microsoft DHCP clients	DC	39-11
lease	Sets the duration an IP address is assigned to a DHCP client	DC	39-11
host*	Specifies the IP address and network mask to manually bind to a DHCP client	DC	39-12
client-identifier*	Specifies a client identifier for a DHCP client	DC	39-13
hardware-address*	Specifies the hardware address of a DHCP client	DC	39-14
clear ip dhcp binding	Deletes an automatic address binding from the DHCP server database	PE	39-14
show ip dhcp binding	Displays address bindings on the DHCP server	PE, NE	39-15

* These commands are used for manua ly binding an address to a client.

service dhcp

This command enables the DHCP server on this switch. Use the **no** form to disable the DHCP server.

Syntax

[**no**] **service dhcp**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

If the DHCP server is running, you must restart it to implement any configuration changes.

Example

```
Console(config)#service dhcp
Console(config)#
```

ip dhcp excluded-address

This command specifies IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

Syntax

[**no**] **ip dhcp excluded-address** *low-address* [*high-address*]

- *low-address* - An excluded IP address, or the first IP address in an excluded address range.
- *high-address* - The last IP address in an excluded address range.

Default Setting

All IP pool addresses may be assigned.

Command Mode

Global Configuration

Example

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```

ip dhcp pool

This command configures a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

Syntax

[**no**] **ip dhcp pool** *name*

name - A string or integer. (Range: 1-8 characters)

Default Setting

DHCP address pools are not configured.

Command Mode

Global Configuration

Usage Guidelines

- After executing this command, the switch changes to DHCP Pool Configuration mode, identified by the (config-dhcp)# prompt.
- From this mode, first configure address pools for the network interfaces (using the **network** command). You can also manually bind an address to a specific

client (with the **host** command) if required. You can configure up to 8 network address pools, and up to 32 manually bound host address pools (i.e., listing one host address per pool). However, note that any address specified in a **host** command must fall within the range of a configured network address pool.

Example

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

Related Commands

network (39-7)
host (39-12)

network

This command configures the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

Syntax

network *network-number* [*mask*]
no network

- *network-number* - The IP address of the DHCP address pool.
- *mask* - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Command Mode

DHCP Pool Configuration

Usage Guidelines

- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used (see page 20-5). The DHCP server assumes that all host addresses are available. You can exclude subsets of the address space by using the ip **dhcp excluded-address** command.

Example

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

default-router

This command specifies default routers for a DHCP pool. Use the **no** form to remove the default routers.

Syntax

default-router *address1* [*address2*]
no default-router

- *address1* - Specifies the IP address of the primary router.
- *address2* - Specifies the IP address of an alternate router.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

The IP address of the router should be on the same subnet as the client. You can specify up to two routers. Routers are listed in order of preference (starting with *address1* as the most preferred router).

Example

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

domain-name

This command specifies the domain name for a DHCP client. Use the **no** form to remove the domain name.

Syntax

domain-name *domain*
no domain-name

domain - Specifies the domain name of the client.
(Range: 1-128 characters)

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

dns-server

This command specifies the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

Syntax

dns-server *address1* [*address2*]
no dns-server

- *address1* - Specifies the IP address of the primary DNS server.
- *address2* - Specifies the IP address of the alternate DNS server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

next-server

This command configures the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

Syntax

[**no**] **next-server** *address*

address - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

Related Commands

bootfile (39-10)

bootfile

This command specifies the name of the default boot image for a DHCP client. This file should placed on the Trivial File Transfer Protocol (TFTP) server specified with the **next-server** command. Use the **no** form to delete the boot image name.

Syntax

bootfile *filename*
no bootfile

filename - Name of the file that is used as a default boot image.

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

Related Commands

next-server (39-9)

netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

Syntax

netbios-name-server *address1* [*address2*]
no netbios-name-server

- *address1* - Specifies IP address of primary NetBIOS WINS name server.
- *address2* - Specifies IP address of alternate NetBIOS WINS name server.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

Servers are listed in order of preference (starting with *address1* as the most preferred server).

Example

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

Related Commands

netbios-node-type (39-11)

netbios-node-type

This command configures the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

Syntax

netbios-node-type *type*
no netbios-node-type

type - Specifies the NetBIOS node type:

- **broadcast**
- **hybrid** (recommended)
- **mixed**
- **peer-to-peer**

Default Setting

None

Command Mode

DHCP Pool Configuration

Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

Related Commands

netbios-name-server (39-10)

lease

This command configures the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

Syntax

lease {*days* [*hours*][*minutes*] | **infinite**}
no lease

- *days* - Specifies the duration of the lease in numbers of days. (Range: 0-364)
- *hours* - Specifies the number of hours in the lease. A *days* value must be supplied before you can configure *hours*. (Range: 0-23)
- *minutes* - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before you can configure *minutes*. (Range: 0-59)
- **infinite** - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client via the **host** command.

Default Setting

One day

Command Modes

DHCP Pool Configuration

Example

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

host

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

Syntax

host *address* [*mask*]
no host

- *address* - Specifies the IP address of a client.
- *mask* - Specifies the network mask of the client.

Default Setting

None

Command Mode

DHCP Pool Configuration

Usage Guidelines

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the switch first checks for a network address pool matching the gateway where the request originated (i.e., if the request was forwarded by a relay server). If there is no gateway in the client request (i.e., the request was not forwarded by a relay server), the switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the **client-identifier** or **hardware-address** commands, then the switch will assign an address from the matching network pool.
- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see page 20-5). This command is valid for manual bindings only.

- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

Example

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

Related Commands

client-identifier (39-13)
hardware-address (39-14)

client-identifier

This command specifies the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

Syntax

client-identifier {**text** *text* | **hex** *hex*}
no client-identifier

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

Default Setting

None

Command Mode

DHCP Pool Configuration

Command Usage

- This command identifies a DHCP client to bind to an address specified in the **host** command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.
- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

Related Commands

host (39-12)

hardware-address

This command specifies the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

Syntax

hardware-address *hardware-address type*
no hardware-address

- *hardware-address* - Specifies the MAC address of the client device.
- *type* - Indicates the following protocol used on the client device:
  - ethernet
  - ieee802
  - fddi

Default Setting

If no type is specified, the default protocol is Ethernet.

Command Mode

DHCP Pool Configuration

Command Usage

This command identifies a DHCP or BOOTP client to bind to an address specified in the **host** command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, you must associate a hardware address with the host entry.

Example

```
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#
```

Related Commands

host (39-12)

clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database.

Syntax

clear ip dhcp binding {*address* | ***** }

- *address* - The address of the binding to clear.
- ***** - Clears all automatic bindings.

Default Setting

None

Command Mode

Privileged Exec

Usage Guidelines

- An *address* specifies the client’s IP address. If an asterisk (*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the **no host** command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

Example.

```
Console#clear ip dhcp binding *
Console#
```

Related Commands

show ip dhcp binding (39-15)

show ip dhcp binding

This command displays address bindings on the DHCP server.

Syntax

show ip dhcp binding [*address*]

address - Specifies the IP address of the DHCP client for which bindings will be displayed.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

```
Console#show ip dhcp binding

     IP                  MAC           Lease Time        Start
                                     (dd/hh/mm/ss)
--------------- ----------------- ------------------ -----------
     192.1.3.21 00-00-e8-98-73-21              86400 Dec 25 08:01:57 2002
Console#
```

Chapter 40: Router Redundancy Commands

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Table 40-1 Router Redundancy Commands

Command Groups	Function	Page
Virtual Router Redundancy Protocol	Configures interface settings for VRRP	40-1

Virtual Router Redundancy Protocol Commands

To configure VRRP, select an interface on each router in the group that will participate in the protocol as the master router or a backup router. To select a specific device as the master router, set the address of this interface as the virtual router address for the group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. You can also enable the preempt feature which allows a router to take over as the master router when it comes on line if it has a higher priority than the currently active master router.

Table 40-2 VRRP Commands

Command	Function	Mode	Page
vrrp ip	Enables VRRP and sets the IP address of the virtual router	IC	40-2
vrrp authentication	Configures a key used to authenticate VRRP packets received from other routers	IC	40-3
vrrp priority	Sets the priority of this router in the VRRP group	IC	40-3
vrrp timers advertise	Sets the interval between successive advertisements by the master virtual router	IC	40-4
vrrp preempt	Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router	IC	40-5
show vrrp	Displays VRRP status information	PE	40-6
show vrrp interface	Displays VRRP status information for the specified interface	PE	40-8
show vrrp router counters	Displays VRRP statistics	PE	40-9
show vrrp interface counters	Displays VRRP statistics for the specified interface	PE	40-9
clear vrrp router counters	Clears VRRP router statistics	PE	40-10
clear vrrp interface counters	Clears VRRP interface statistics	PE	40-10

vrrp ip

This command enables the Virtual Router Redundancy Protocol (VRRP) on an interface and specifies the IP address of the virtual router. Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

Syntax

[**no**] **vrrp** *group* **ip** *ip-address*

- *group* - Identifies the virtual router group. (Range: 1-255)
- *ip-address* - The IP address of the virtual router. This is the IP address that end-hosts set as their default gateway.

Default Setting

No virtual router groups are configured.

Command Mode

Interface (VLAN)

Command Usage

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- If the IP address assigned to the virtual router with this command is already configured as the primary address on this interface, this router is considered the Owner, and will assume the role of the Master virtual router in the group.
- This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when operating as the Master VRRP router.
- VRRP is enabled as soon as this command is entered. If you need to customize any of the other parameters for VRRP such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

Example

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#
```

vrrp authentication

This command specifies the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

Syntax

vrrp *group* **authentication** *key*
no vrrp *group* **authentication**

- *group* - Identifies the virtual router group. (Range: 1-255)
- *key* - Authentication string. (Range: 1-8 alphanumeric characters)

Default Setting

No key is defined.

Command Mode

Interface (VLAN)

Command Usage

- All routers in the same VRRP group must be configured with the same authentication key.
- When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.
- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

Example

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

vrrp priority

This command sets the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

Syntax

vrrp *group* **priority** *level*
no vrrp *group* **priority**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *level* - Priority of this router in the VRRP group. (Range: 1-254)

Default Setting

Master: 255
Backup: 100

Command Mode

Interface (VLAN)

Command Usage

- A router that has a physical interface with the same IP address as that used for the virtual router (that is, the owner of the VRRP IP address) will become the master virtual router. The backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.
- If two or more routers are configured with the same VRRP priority, the router with the highest IP address is elected as the new master router if the current master fails.
- If the backup preempt function is enabled with the **vrrp preempt** command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- If the virtual IP address for the VRRP group is the same as that of the configured device, the priority will automatically be set to 255 prior to using this command.

Example

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

Related Commands

vrrp preempt (40-5)

vrrp timers advertise

This command sets the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

Syntax

vrrp *group* **timers advertise** *interval*
no vrrp *group* **timers advertise**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *interval* - Advertisement interval for the master virtual router. (Range: 1-255 seconds)

Default Setting

1 second

Command Mode

Interface (VLAN)

Command Usage

- VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
- VRRP advertisements are sent to the multicast address 224.0.0.18. Using a multicast address reduces the amount of traffic that has to processed by network devices that are not part of the designated VRRP group.
- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second

Example

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

vrrp preempt

This command configures the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

Syntax

vrrp *group* **preempt** [**delay** *seconds*]
no vrrp *group* **preempt**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *seconds* - The time to wait before issuing a claim to become the master. (Range: 0-120 seconds)

Default Setting

Preempt: Enabled
Delay: 0 seconds

Command Mode

Interface (VLAN)

Command Usage

- If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However, note that if the original master (i.e., the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the

master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

Example

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

Related Commands

vrrp priority (40-3)

show vrrp

This command displays status information for VRRP.

Syntax

show vrrp [**brief** | *group*]

- **brief** - Displays summary information for all VRRP groups on this router.
- *group* - Identifies a VRRP group. (Range: 1-255)

Defaults

None

Command Mode

Privileged Exec

Command Usage

- Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- Specify a group number to display status information for a specific group

Example

This example displays the full listing of status information for all groups.

```
Console#show vrrp
 Vlan 1 - Group 1,
 State                            Master
 Virtual IP Address               192.168.1.6
 Virtual MAC Address              00-00-5E-00-01-01
 Advertisement Interval           5 sec
 Preemption                       Enabled
 Min Delay                        10 sec
 Priority                         1
 Authentication                   SimpleText
 Authentication Key               bluebird
 Master Router                    192.168.1.6
 Master Priority                  255
 Master Advertisement Interval    5 sec
 Master Down Interval             15
Console#
```

Table 40-3 show vrrp - display description

Field	Description
State	VRRP role of this interface (master or backup)
Virtual IP address	Virtual address that identifies this VRRP group
Virtual MAC address	Virtual MAC address derived from the owner of the virtual IP address
Advertisement interval	Interval at which the master virtual router advertises its role as the master
Preemption	Shows whether or not a higher priority router can preempt the current acting master
Min delay	Delay before a router with a higher priority can preempt the current acting master
Priority	Priority of this router
Authentication	Authentication mode used to verify VRRP packets
Authentication key	Key used to authenticate VRRP packets received from other routers
Master Router	IP address of the router currently acting as the VRRP group master
Master priority	The priority of the router currently acting as the VRRP group master
Master Advertisement interval	The advertisement interval configured on the VRRP master.
Master down interval	The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings)

This example displays the brief listing of status information for all groups.

```
Console#show vrrp brief
Interface   Grp    State    Virtual addr     Int   Pre   Prio
----------------------------------------------------------------
vlan 1      1      Master   192.168.1.6      5      E    1
Console#
```

Table 40-4 show vrrp brief - display description

Field	Description
Interface	VLAN interface
Grp	VRRP group
State	VRRP role of this interface (master or backup)
Virtual addr	Virtual address that identifies this VRRP group
Int	Interval at which the master virtual router advertises its role as the master
Pre	Shows whether or not a higher priority router can preempt the current acting master
Prio	Priority of this router

show vrrp interface

This command displays status information for the specified VRRP interface.

Syntax

show vrrp interface vlan *vlan-id* [**brief**]

- *vlan-id* - Identifier of configured VLAN interface. (Range: 1-4093)
- **brief** - Displays summary information for all VRRP groups on this router.

Defaults

None

Command Mode

Privileged Exec

Example

This example displays the full listing of status information for VLAN 1.

```
Console#show vrrp interface vlan 1
 Vlan 1 - Group 1,
 State                            Master
 Virtual IP Address               192.168.1.6
 Virtual MAC Address              00-00-5E-00-01-01
 Advertisement Interval           5 sec
 Preemption                       enabled
 Min Delay                        10 sec
 Priority                         1
 Authentication                   SimpleText
 Authentication Key               bluebird
 Master Router                    192.168.1.6
 Master Priority                  1
 Master Advertisement Interval    5 sec
 Master Down Interval             15
Console#
```

* Refer to “show vrrp” on page 40-6 for a description of the display items.

show vrrp router counters

This command displays counters for errors found in VRRP protocol packets.

Command Mode

Privileged Exec

Example

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```
Console#show vrrp router counters
 Total Number of VRRP Packets with Invalid Checksum : 0
 Total Number of VRRP Packets with Unknown Error    : 0
 Total Number of VRRP Packets with Invalid VRID     : 0
Console#
```

show vrrp interface counters

This command displays counters for VRRP protocol events and errors that have occurred for the specified group and interface.

show vrrp *group* **interface vlan** *interface* **counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4093)

Defaults

None

Command Mode

Privileged Exec

Example

```
Console#show vrrp 1 interface vlan 1 counters
 Total Number of Times Transitioned to MASTER                           : 6
 Total Number of Received Advertisements Packets                        : 0
 Total Number of Received Error Advertisement Interval Packets          : 0
 Total Number of Received Authentication Failures Packets               : 0
 Total Number of Received Error IP TTL VRRP Packets                     : 0
 Total Number of Received Priority 0 VRRP Packets                       : 0
 Total Number of Sent Priority 0 VRRP Packets                           : 5
 Total Number of Received Invalid Type VRRP Packets                     : 0
 Total Number of Received Error Address List VRRP Packets               : 0
 Total Number of Received Invalid Authentication Type VRRP Packets      : 0
 Total Number of Received Mismatch Authentication Type VRRP Packets     : 0
 Total Number of Received Error Packet Length VRRP Packets              : 0
Console#
```

* Refer to “Displaying VRRP Group Statistics” on page 18-8 for a description of the display items.

clear vrrp router counters

This command clears VRRP system statistics.

Command Mode

Privileged Exec

Example

```
Console#clear vrrp router counters
Console#
```

clear vrrp interface counters

This command clears VRRP system statistics for the specified group and interface.

clear vrrp *group* **interface** *interface* **counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4093)

Defaults

None

Command Mode

Privileged Exec

Example

```
Console#clear vrrp 1 interface 1 counters
Console#
```

Chapter 41: IP Interface Commands

An IP address may be used for management access to the router over your network or to connect the switch to existing IP subnets. An IPv4 address is obtained via DHCP by default for VLAN 1. You can also manually configure a new address for other VLANs on the router to enable management access through these VLANs or to connect the router to existing IP subnets. You can manually configure a specific IPv4 or IPv6 address, or direct the router to obtain an IPv4 address from a BOOTP or DHCP server when it is powered on. Both IP Version 4 and 6 addresses can be defined and used simultaneously to access the router. An IPv6 address can either be manually configured or dynamically generated. You may also need to a establish an IPv4 or IPv6 default gateway between this device and management stations or other devices that exist on another network segment (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP. These commands are used to connect subnetworks to the enterprise network.

Table 41-1 IP Interface Commands

Command Group	Function	Page
Basic IP Configuration	Configures the IP address for interfaces and the gateway router	41-1
Address Resolution Protocol (ARP)	Configures static, dynamic and proxy ARP service	41-32

Basic IP Configuration

This section describes commands used to configure IP addresses for VLAN interfaces on the switch.

Table 41-2 Basic IP Configuration Commands

Command	Function	Mode	Page
IP Version 4			
ip address	Sets the IP address for the current interface	IC	41-3
ip default-gateway	Defines the default gateway through which this router can reach other subnetworks	GC	41-4
show ip interface	Displays the IP settings for this device	PE	41-5
show ip redirects	Displays the default gateway configured for this device	PE	41-5
ping	Sends ICMP echo request packets to another node on the network	NE, PE	41-6

Table 41-2 Basic IP Configuration Commands (Continued)

Command	Function	Mode	Page
IP Version 6			
Interface Address Configuration and Utilities			
ipv6 enable	Enables IPv6 on an interface that has not been configured with an explicit IPv6 address	IC	41-7
ipv6 general-prefix	Defines an IPv6 general prefix for the network address segment	GC	41-8
show ipv6 general-prefix	Displays all configured IPv6 general prefixes	NE, PE	41-9
ipv6 address	Configures an IPv6 global unicast address with an option to use an IPv6 general prefix, and enables IPv6 on an interface	IC	41-9
ipv6 address autoconfig	Enables automatic configuration of IPv6 global unicast addresses on an interface and enables IPv6 on the interface	IC	41-10
ipv6 address eui-64	Configures an IPv6 global unicast address for an interface using an EUI-64 interface ID in the low order 64 bits, and enables IPv6 on the interface	IC	41-12
ipv6 address link-local	Configures an IPv6 link-local address for an interface and enables IPv6 on the interface	IC	41-13
show ipv6 interface	Displays the usability and configured settings for IPv6 interfaces	NE, PE	41-14
ipv6 default-gateway	Sets an IPv6 default gateway for traffic with no known next hop	GC	41-17
show ipv6 default-gateway	Displays the current IPv6 default gateway	NE, PE	41-17
ipv6 mtu	Sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface	IC	41-18
show ipv6 mtu	Displays maximum transmission unit (MTU) information for IPv6 interfaces	NE, PE	41-19
show ipv6 traffic	Displays statistics about IPv6 traffic	NE, PE	41-19
clear ipv6 traffic	Resets IPv6 traffic counters	PE	41-25
ping ipv6	Sends ICMP echo request packets to an IPv6 node on the network	NE, PE	41-25
Neighbor Discovery			
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache	GC	41-26
ipv6 nd dad attempts	Configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection	IC	41-27
ipv6 nd ns interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface	IC	41-29
show ipv6 neighbors	Displays information in the IPv6 neighbor discovery cache	NE, PE	41-30
clear ipv6 neighbors	Deletes all dynamic entries in the IPv6 neighbor discovery cache	PE	41-31

ip address

This command sets the IPv4 address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

Syntax

ip address {*ip-address netmask* | **bootp** | **dhcp**} [*secondary*]
no ip address

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.
- *secondary* - Specifies a secondary IP address.

Default Setting

DHCP

Command Mode

Interface Configuration (VLAN)

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes via shared media) that will be assigned to a specific subnet, then create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router’s host number on that network. In other words, a router interface address defines the network segment that is connected to that interface, and allows IP packets to be sent to or from the router.
- Before any network interfaces are configured on the router, first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- An IP address must be assigned to this device to gain management access over the network or to connect the router to existing IP subnets. A specific IP address can be manually configured, or the router can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything outside this format will not be accepted by the configuration program.
- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface. Note that a secondary address cannot be configured prior to setting the primary IP address, and the primary address cannot be removed if a secondary address is still present. Also, if any router in a network segment

uses a secondary address, all other routers in that segment must also use a secondary address from the same network or subnet address space.

- If **bootp** or **dhcp** options are selected, the system will immediately start broadcasting service requests. IP is enabled but will not function until a BOOTP or DHCP reply has been received. Requests will be broadcast periodically by this device in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- BOOTP or DHCP requests can be broadcast for all VLANs configured to obtain address assignments through BOOTP or DHCP by entering the **ip dhcp restart client** command, or by rebooting the router.

Note: Each VLAN group can be assigned its own IP interface address. Therefore, if routing is enabled, you can manage the router via any of these IP addresses.

Example

In the following example, the device is assigned an address in VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

Related Commands

ip dhcp restart client (39-2)
ipv6 address (41-9)

ip default-gateway

This command specifies the IPv4 default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

Syntax

ip default-gateway *gateway*
no ip default-gateway

gateway - IP address of the default gateway

Default Setting

No static route is established.

Command Mode

Global Configuration

Command Usage

- The gateway specified in this command is only valid if routing is disabled with the **no ip routing** command (page 42-1). If IP routing is disabled, you must define a gateway if the target device is located in a different subnet.
- If routing is enabled, you can still define a static route using the **ip route** command (page 42-2) to ensure that traffic to the designated address or subnet passes through a preferred gateway.

Example

The following example defines a default gateway for this device:

```
Console(config)#ip default-gateway 10.1.1.254
Console(config)#
```

Related Commands

ip route (42-2)
show ip redirects (41-5)
ipv6 default-gateway (41-17)

show ip interface

This command displays the settings of an IPv4 interface.

Command Mode

Privileged Exec

Example

```
Console#show ip interface

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.0.2, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is disabled

Console#
```

Related Commands

ip address (41-3)
show ipv6 interface (41-14)

show ip redirects

This command shows the IPv4 default gateway configured for this device.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

Related Commands

ip default-gateway (41-4)
show ipv6 default-gateway (41-17)

ping

This command sends (IPv4) ICMP echo request packets to another node on the network.

Syntax

ping *host* [**size** *size*] [**count** *count*]

- *host* - IP address or IP alias of the host.
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)
  The actual packet size will be eight bytes larger than the size specified because the router adds header information.
- *count* - Number of packets to send. (Range: 1-16, default: 5)

Default Setting

size: 32 bytes
count: 5

Command Mode

Normal Exec, Privileged Exec

Command Usage

- Use the ping command to see if another site on the network can be reached.
- The following are some results of the **ping** command:
  - *Normal response* - The normal response occurs in one to ten seconds, depending on network traffic.
  - *Destination does not respond* - If the host does not respond, a “timeout” appears in ten seconds.
  - *Destination unreachable* - The gateway for this destination indicates that the destination is unreachable.
  - *Network or host unreachable* - The gateway found no corresponding entry in the route table.
- When pinging a host name, be sure the DNS server has been enabled (see page 38-5). If necessary, local devices can also be specified in the DNS static host table (see page 38-1).

Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5 seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

Related Commands

interface (27-1)
ping ipv6 (41-25)

ipv6 enable

This command enables IPv6 on an interface that has not been configured with an explicit IPv6 address. Use the **no** form to disable IPv6 on an interface that has not been configured with an explicit IPv6 address.

Syntax

[**no**] **ipv6 enable**

Default Setting

IPv6 is disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- This command enables IPv6 on the current VLAN interface and automatically generates a link-local unicast address. The address prefix uses FE80, and the host portion of the address is generated by converting the router’s MAC address to modified EUI-64 format (see page 41-12). This address type makes the router accessible over IPv6 for all devices attached to the same local subnet.
- If a duplicate address is detected on the local segment, this interface will be disabled and a warning message displayed on the console.
- The **no ipv6 enable** command does not disable IPv6 for an interface that has been explicitly configured with an IPv6 address.

Example

In this example, IPv6 is enabled on VLAN 1, and the link-local address FE80::200:E8FF:FE90:0/64 is automatically generated by the router.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 enable
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Related Commands

ipv6 address link-local (41-13)
show ipv6 interface (41-14)

ipv6 general-prefix

This command defines an IPv6 general prefix for the network address segment. Use the **no** form to remove the IPv6 general prefix.

Syntax

ipv6 general-prefix *prefix-name ipv6-prefix*/*prefix-length*
no ipv6 general-prefix *prefix-name*

- *prefix-name* - The label assigned to the general prefix.
- *ipv6-prefix* - The high-order bits of the network address segment assigned to the general prefix. The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- *prefix-length* - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No general prefix is defined

Command Mode

Global Configuration

Command Usage

- Prefixes may contain zero-value fields or end in zeros.
- A general prefix holds a short prefix that indicates the high-order bits used in the network portion of the address. Longer, more specific, prefixes can be based on the general prefix to specify any number of subnets. When the general prefix is changed, all of the more specific prefixes based on this prefix will also change.

Example

This example assigns a general network prefix of 2009:DB9:2229::/48 to the router.

```
Console(config)#ipv6 general-prefix rd 2009:DB9:2229::/48
Console(config)#end
Console#show ipv6 general-prefix
IPv6 general prefix: rd
2009:DB9:2229::/48
Console#
```

Related Commands

show ipv6 general-prefix (41-9)

show ipv6 general-prefix

This command displays all configured IPv6 general prefixes.

Command Mode

Normal Exec, Privileged Exec

Example

This example displays a single IPv6 general prefix configured for the router.

```
Console#show ipv6 general-prefix
IPv6 general prefix: rd
2009:DB9:2229::/48
Console#
```

ipv6 address

This command configures an IPv6 global unicast address and enables IPv6 on an interface. Use the **no** form without any arguments to remove all IPv6 addresses from the interface, or use the **no** form with a specific IPv6 address to remove that address from the interface.

Syntax

ipv6 address [*general-prefix-name*] *ipv6-address*/*prefix-length*
no ipv6 address [[*general-prefix-name*] *ipv6-address*/*prefix-length*]]

- *general-prefix-name* - The label assigned to the general prefix which specifies the leading bits of the network portion of the address.
- *ipv6-address* - A full IPv6 address if no general prefix is used, or the subsequent bits following the general prefix if one is used followed by the host address bits. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- *prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address). The length of this prefix includes both the general prefix and any number of subsequent IPv6 prefix bits specified in this command. If the prefix length specified by this command is shorter than the general prefix, then the length of the general prefix takes precedence.

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- The general prefix normally applies to all interfaces, and is therefore specified at the global configuration level. The subsequent network prefix bits normally apply to one or more specific interfaces, and are therefore specified by this command at the interface configuration level.

- If a link-local address has not yet been assigned to this interface, this command will assign the specified static global unicast address and also dynamically generate a link-local unicast address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the router’s MAC address in modified EUI-64 format.)
- If a duplicate address is detected, a warning message is sent to the console.

Example

This example uses the general network prefix of 2009:DB9:2229::/48 used in an earlier example, and then specifies the subsequent prefix bits 0:0:0:7279::/64, and finally the host address portion of 79.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address rd 0:0:0:7279::79/64
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229:7279::79, subnet is 2009:DB9:2229:7279::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Related Commands

ipv6 address eui-64 (41-12)
ipv6 address autoconfig (41-10)
show ipv6 interface (41-14)
ip address (41-3)

ipv6 address autoconfig

This command enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages; the host portion in based on the modified EUI-64 form of the interface identifier (i.e., the router’s MAC address). Use the **no** form to remove the address generated by this command.

Syntax

[**no**] **ipv6 address autoconfig**

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link local address for the interface. (The link-local address is made with an address prefix of FE80 and a host portion based the router's MAC address in modified EUI-64 format.)
- If a duplicate address is detected, a warning message is sent to the console.
- If the router advertisements have the "other stateful configuration" flag set, the router will attempt to acquire other non-address configuration information (such as a default gateway) from a DHCP for IPv6 server.

Example

This example assigns two dynamic global unicast address of 2005::212:CFFF:FE0B:4600 and 3FFE:501:FFFF:100:212:CFFF:FE0B:4600 to the router.

```
Console(config-if)#ipv6 address autoconfig
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::212:CFFF:FE0B:4600/64
Global unicast address(es):
  2005::212:CFFF:FE0B:4600, subnet is 2005:0:0:0::/64
  3FFE:501:FFFF:100:212:CFFF:FE0B:4600, subnet is 3FFE:501:FFFF:100::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF0B:4600/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Related Commands

ipv6 address (41-9)
show ipv6 interface (41-14)

ipv6 address eui-64

This command configures an IPv6 address for an interface using an EUI-64 interface ID in the low order 64 bits and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

Syntax

ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**
no ipv6 address [*ipv6-prefix*/*prefix-length* **eui-64**]

- *ipv6-prefix* - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- *prefix-length* - A decimal value indicating how many contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- If a link local address has not yet been assigned to this interface, this command will dynamically generate a global unicast address and a link-local address for this interface. (The link-local address is made with an address prefix of FE80 and a host portion based the router’s MAC address in modified EUI-64 format.)
- Note that the value specified in the ipv6-prefix may include some of the high-order host bits if the specified prefix length is less than 64 bits. If the specified prefix length exceeds 64 bits, then the network portion of the address will take precedence over the interface identifier.
- If a duplicate address is detected, a warning message is sent to the console.
- IPv6 addresses are 16 bytes long, of which the bottom 8 bytes typically form a unique host identifier based on the device’s MAC address. The EUI-64 specification is designed for devices that use an extended 8-byte MAC address. For devices that still use a 6-byte MAC address (also known as EUI-48 format), it must be converted into EUI-64 format by inverting the universal/local bit in the address and inserting the hexadecimal number FFFE between the upper and lower three bytes of the of the MAC address.

  For example, if a device had an EUI-48 address of 28-9F-18-1C-82-35, the global/local bit must first be inverted to meet EUI-64 requirements (i.e., 1 for globally defined addresses and 0 for locally defined addresses), changing 28 to 2A. Then the two bytes FFFE are inserted between the OUI (i.e., company id) and the rest of the address, resulting in a modified EUI-64 interface identifier of 2A-9F-18-FF-FE-1C-82-35.

- This host addressing method allows the same interface identifier to be used on multiple IP interfaces of a single device, as long as those interfaces are attached to different subnets.

Example

This example uses the general network prefix of 2001:0DB8:0:1::/64 used in an earlier example, and specifies that the EUI-64 interface identifier be used in the lower 64 bits of the address.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address 2001:0DB8:0:1::/64 eui-64
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2001:DB8::1:200:E8FF:FE90:0, subnet is 2001:DB8:0:1::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Related Commands

ipv6 address autoconfig (41-10)
show ipv6 interface (41-14)

ipv6 address link-local

This command configures an IPv6 link-local address for an interface and enables IPv6 on the interface. Use the **no** form without any arguments to remove all manually configured IPv6 addresses from the interface. Use the **no** form with a specific address to remove it from the interface.

Syntax

ipv6 address *ipv6-address* **link-local**
no ipv6 address [*ipv6-address* **link-local**]

ipv6-address - The IPv6 address assigned to the interface. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields. And the address prefix must be FE80.

Default Setting

No IPv6 addresses are defined

Command Mode

Interface Configuration (VLAN)

Command Usage

- The address specified with this command replaces a link-local address that was automatically generated for the interface.
- You can configure multiple IPv6 global unicast addresses per interface, but only one link-local address per interface.
- If a duplicate address is detected, a warning message is sent to the console.

Example

This example assigns a link-local address of FE80::269:3EF9:FE19:6779 to VLAN 1. Note that the prefix FE80 is required for link-local addresses, and the first 16-bit group in the host address is padded with a zero in the form 0269.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 address FE80::269:3EF9:FE19:6779 link-local
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2001:DB8::1:200:E8FF:FE90:0, subnet is 2001:DB8:0:1::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF19:6779/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Related Commands

ipv6 enable (41-7)
show ipv6 interface (41-14)

show ipv6 interface

This command displays the usability and configured settings for IPv6 interfaces.

Syntax

show ipv6 interface [**brief** [**vlan** *vlan-id* [*ipv6-prefix*/*prefix-length*]]]

- **brief** - Displays a brief summary of IPv6 operational status and the addresses configured for each interface.
- *vlan-id* - VLAN ID (Range: 1-4093)
- *ipv6-prefix* - The IPv6 network portion of the address assigned to the interface. The prefix must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal

values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

- *prefix-length* - A decimal value indicating how many of the contiguous bits (from the left) of the address comprise the prefix (i.e., the network portion of the address).

Command Mode

Normal Exec, Privileged Exec

Example

This example displays all the IPv6 addresses configured for the router.

```
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::269:3EF9:FE19:6779/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF19:6779/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 1.
ND retransmit interval is 1000 milliseconds
Console#
```

Table 41-3 show ipv6 interface - display description

Field	Description
VLAN	A VLAN is marked “up” if the router can send and receive packets on this interface, “down” if a line signal is not present, or “administratively down” if the interface has been disabled by the administrator.
IPv6	IPv6 is marked “enable” if the router can send and receive IP traffic on this interface, “disable” if the router cannot send and receive IP traffic on this interface, or “stalled” if a duplicate link-local address is detected on the interface.
Link-local address	Shows the link-local address assigned to this interface
Global unicast address(es)	Shows the global unicast address(es) assigned to this interface

Table 41-3 show ipv6 interface - display description (Continued)

Field	Description
Joined group address(es)	In addition to the unicast addresses assigned to an interface, a node is required to join the all-nodes multicast addresses FF01::1 and FF02::1 for all IPv6 nodes within scope 1 (interface-local) and scope 2 (link-local), respectively. FF01::1/16 is the transient node-local multicast address for all attached IPv6 nodes, and FF02::1/16 is the link-local multicast address for all attached IPv6 nodes. The node-local multicast address is only used for loopback transmission of multicast traffic. Link-local multicast addresses cover the same types as used by link-local unicast addresses, including all nodes (FF02::1), all routers (FF02::2), and solicited nodes (FF02::1:FFXX:XXXX) as described below. A node is also required to compute and join the associated solicited-node multicast addresses for every unicast and anycast address it is assigned. IPv6 addresses that differ only in the high-order bits, e.g. due to multiple high-order prefixes associated with different aggregations, will map to the same solicited-node address, thereby reducing the number of multicast addresses a node must join. In this example, FF02::1:FF90:0/104 is the solicited-node multicast address which is formed by taking the low-order 24 bits of the address and appending those bits to the prefix.
MTU	Maximum transmission unit for this interface.
ND DAD	Indicates whether (neighbor discovery) duplicate address detection is enabled.
number of DAD attempts	The number of consecutive neighbor solicitation messages sent on the interface during duplicate address detection.

This example displays a brief summary of IPv6 addresses configured on the router.

```
Console#show ipv6 interface brief
Vlan 1 is up
IPv6 is enable.
  FF01::1
  2009:DB9:2229::79
  FE80::269:3EF9:FE19:6779
  FF02::1
  FF02::1:FF00:79
  FF02::1:FF19:6779
Console#
```

Related Commands

show ip interface (41-5)

ipv6 default-gateway

This command sets an IPv6 default gateway to use for destinations with no known next hop. Use the **no** form to remove a previously configured default gateway.

Syntax

ipv6 default-gateway *ipv6-address*
no ipv6 address

ipv6-address - The IPv6 address of the default next hop router to use when no other routing information is known about an IPv6 address. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

No default gateway is defined

Command Mode

Global Configuration

Command Usage

- The gateway specified in this command is only valid if routing is disabled with the **no ip routing** command. If IP routing is disabled, you must define a gateway if the target device is located in a different subnet.
- If routing is enabled, you can still define a static route using the **ip route** command (page 42-2) to ensure that traffic to the designated address or subnet passes through a preferred gateway.
- An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the router.

Example

The following example defines a default gateway for this device:

```
Console(config)#ipv6 default-gateway EE80::269:3EF9:FE19:6780
Console(config)#
```

Related Commands

show ipv6 default-gateway (41-17)
ip default-gateway (41-4)

show ipv6 default-gateway

This command displays the current IPv6 default gateway.

Command Mode

Normal Exec, Privileged Exec

Example

The following shows the default gateway configured for this device:

```
Console#show ipv6 default-gateway
ipv6 default gateway:  FE80::269:3EF9:FE19:6780
Console#
```

Related Commands

show ip redirects (41-5)

ipv6 mtu

This command sets the size of the maximum transmission unit (MTU) for IPv6 packets sent on an interface. Use the **no** form to restore the default setting.

Syntax

ipv6 mtu *size*
no ipv6 mtu

size - Specifies the MTU size. (Range: 1280-65535 bytes)

Default Setting

1500 bytes

Command Mode

Interface Configuration (VLAN)

Command Usage

- If a non-default value is configured, an MTU option is included in the router advertisements sent from this device. This option is provided to ensure that all nodes on a link use the same MTU value in cases where the link MTU is not otherwise well known.
- IPv6 routers do not fragment IPv6 packets forwarded from other routers. However, traffic originating from an end-station connected to an IPv6 router may be fragmented.
- All devices on the same physical medium must use the same MTU in order to operate correctly.
- IPv6 must be enabled on an interface before the MTU can be set.

Example

The following example sets the MTU for VLAN 1 to 1280 bytes:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 mtu 1280
Console(config-if)#
```

Related Commands

show ipv6 mtu (41-19)
jumbo frame (23-9)

show ipv6 mtu

This command displays the maximum transmission unit (MTU) cache for destinations that have returned an ICMP packet-too-big message along with an acceptable MTU to this router.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows the MTU cache for this device:

```
Console#show ipv6 mtu
MTU       Since    Destination Address
1400      00:04:21   5000:1::3
1280       00:04:50   FE80::203:A0FF:FED6:141D
Console#
```

Table 41-4 show ipv6 mtu - display description

Field	Description
MTU	Adjusted MTU contained in the ICMP packet-too-big message returned from this destination, and now used for all traffic sent along this path.
Since	Time since an ICMP packet-too-big message was received from this destination.
Destination Address	Address which sent an ICMP packet-too-big message.

show ipv6 traffic

This command displays statistics about IPv6 traffic passing through this router.

Command Mode

Normal Exec, Privileged Exec

Example

The following example shows statistics for all IPv6 unicast and multicast traffic, as well as ICMP, UDP and TCP statistics:

```
Console#show ipv6 traffic
IPv6 Statistics:
Ipv6 rcvd
        rcvd total               1432
        source routed           0
        truncated               0
        format errors           0
        hop count exceeded      0
        unknown protocol        0
        not a router            0
        fragments               0
        total reassembled       0
        reassembly timeouts     0
        reassembly failures     0
Ipv6 sent
        sent generated          1435
        forwarded               0
        fragmented              0
        generated fragments     0
        Fragmented failed       0
        encapsulation failed    0
        no route                0
        too big                 0
Ipv6 mcast
        mcast received          0
        mcast sent              2
ICMP Statistics:
Ipv6 icmp input
        input                   1
        checksum errors         0
        too short               0
        unknown info type       0
        unknown error type      0
        unreach routing         0
        unreach admin           0
        unreach neighbor        0
        unreach address         0
        unreach port            1
        Parameter error         0
        Parameter header        0
        Parameter option        0
        hopcount expired        0
        reassembly timeout      0
        too big                 0
        echo request            0
        echo reply              0
        group query             0
        group report            0
        group reduce            0
        router solicit          0
        router advert           0
        redirects               0
        neighbor solicit        0
        neighbor advert         0
Ipv6 icmp output
        sent output             6
        unreach routing         0
        unreach admin           0
        unreach neighbor        0
        unreach address         0
        unreach port            1
        parameter error         0
        parameter header        0
        parameter option        0
        hopcount expired        0
        Reassembly timeout      0
        too big                 0
        echo request            0
        echo reply              0
        group query             0
        group report            1
        group reduce            0
        router solicit          0
        router advert           0
        redirects               0
        neighbor solicit        1
        neighbor advert         0
```

```
UDP Statistics:
        input                   1
        checksum errors         0
        length errors           0
        no port                 1
        dropped                 0
        output                  1
TCP Statistics:
        input                   1911
        checksum errors         0
        output                  4339
        retransmitted           0

Console#
```

Table 41-5   show ipv6 traffic - display description

Field	Description
IPv6 Statistics	
Ipv6 rcvd	
rcvd total	The total number of input datagrams received by the interface, including those received in error.
source routed	The number of source-routed packets.
truncated	The number of input datagrams discarded because the datagram frame did not carry enough data.
format errors	The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatches, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc.
hop count exceeded	Number of packets discarded because its time-to-live (TTL) field was decremented to zero.
unknown protocol	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.
not a router	The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
fragments	The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
total reassembled	The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.
reassembly timeouts	The number of times the reassembly of a packet timed out.

Table 41-5 show ipv6 traffic - display description (Continued)

Field	Description
reassembly failures	The number of failures detected by the IPv6 re-assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.
Ipv6 sent	
sent generated	The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in ipv6IfStatsOutForwDatagrams.
forwarded	The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram, the counter of the outgoing interface is incremented.
fragmented	The number of IPv6 datagrams that have been successfully fragmented at this output interface.
generated fragments	The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.
fragmented failed	The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.
encapsulation failed	Failure that can result from an unresolved address or failure to queue a packet.
no route	The number of input datagrams discarded because no route could be found to transmit them to their destination.
too big	The number of input datagrams that could not be forwarded because their size exceeded the link MTU of the outgoing interface.
Ipv6 mcast	
mcast received	The number of multicast packets received by the interface.
mcast sent	The number of multicast packets transmitted by the interface.
ICMP Statistics	
Ipv6 icmp input	
input	The total number of ICMP messages received by the interface which includes all those counted by ipv6IfIcmpInErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages.
checksum errors	The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).
too short	Packet length is too short.
unknown info type	ICMPv6 information message not defined in the standards.
unknown error type	ICMPv6 error message not defined in the standards.
unreach routing	The number of times no route was found to the destination.

Table 41-5 show ipv6 traffic - display description (Continued)

Field	Description
unreach admin	The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.
unreach neighbor	Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source.
unreach address	The number of times that an address is unreachable.
unreach port	The number of times that a port is unreachable.
parameter error	The number of ICMP Parameter Problem messages received by the interface.
parameter header	The number of Receive ICMP parameter problem messages caused by an unrecognized header error.
parameter option	The number of Receive ICMP parameter problem messages caused by an unrecognized option error.
hopcount expired	The number of Receive ICMP parameter problem messages caused by the hop limit being exceeded in transit.
reassembly timeout	The number of Receive ICMP parameter problem messages caused by the fragment reassembly time being exceeded.
too big	The number of ICMP Packet Too Big messages received by the interface.
echo request	The number of ICMP Echo (request) messages received by the interface.
echo reply	The number of ICMP Echo Reply messages received by the interface.
group query	The number of ICMPv6 Group Membership Query messages received by the interface.
group report	The number of ICMPv6 Group Membership Response messages received by the interface.
group reduce	The number of ICMPv6 Group Membership Reduction messages received by the interface.
router solicit	The number of ICMP Router Solicit messages received by the interface.
router advert	The number of ICMP Router Advertisement messages received by the interface.
redirects	The number of Redirect messages received.
neighbor solicit	The number of ICMP Neighbor Solicitation messages received by the interface.
neighbor advert	The number of ICMP Neighbor Advertisement messages received by the interface.
Ipv6 icmp output	
sent output	The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.
unreach routing	The number of times no route was found to the destination.
unreach admin	The number of ICMP destination unreachable/communication administratively prohibited messages sent by the interface.
unreach neighbor	Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source.
unreach address	The number of times that an address is unreachable.
unreach port	The number of times that a port is unreachable.

Table 41-5 show ipv6 traffic - display description (Continued)

Field	Description
parameter error	The number of ICMP Parameter Problem messages sent by the interface.
parameter header	The number of Send ICMP parameter problem messages caused by an unrecognized header error.
parameter option	The number of Send ICMP parameter problem messages caused by an unrecognized option error.
hopcount expired	The number of Send ICMP parameter problem messages caused by the hop limit being exceeded in transit.
reassembly timeout	The number of Send ICMP parameter problem messages caused by the fragment reassembly time being exceeded.
too big	The number of ICMP Packet Too Big messages sent by the interface.
echo request	The number of ICMP Echo (request) messages sent by the interface.
echo reply	The number of ICMP Echo Reply messages sent by the interface.
group query	The number of ICMPv6 Group Membership Query messages sent.
group report	The number of ICMPv6 Group Membership Response messages sent.
group reduce	The number of ICMPv6 Group Membership Reduction messages sent.
router solicit	The number of ICMP Router Solicitation messages sent by the interface.
router advert	The number of ICMP Router Advertisement messages sent by the interface.
redirects	The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.
neighbor solicit	The number of ICMP Neighbor Solicitation messages sent by the interface.
neighbor advert	The number of ICMP Neighbor Advertisement messages sent by the interface.
UDP Statistics	
input	The total number of UDP datagrams delivered to UDP users.
checksum errors	The total number of UDP packet checksum errors.
length errors	The total number of UDP header length errors.
no port	The total number of received UDP datagrams for which there was no application at the destination port.
dropped	The number of times the system encounter an error when trying to queue the received packet.
output	The total number of UDP datagrams sent from this entity.
TCP Statistics	
input	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
checksum errors	The total number of TCP packet checksum errors.
output	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
retransmitted	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

clear ipv6 traffic

This command resets IPv6 traffic counters.

Command Mode

Privileged Exec

Command Usage

This command resets all of the counters displayed by the **show ipv6 traffic** command.

Example

```
Console#clear ipv6 traffic
Console#
```

ping ipv6

This command sends ICMP echo request packets to an IPv6 node on the network.

ping ipv6 address {*ipv6-address* | *host-name*} [**size** *datagram-size* | **repeat** *repeat-count* | **data** *hex-data-pattern* | **source** *source-address* | **timeout** *seconds* | **verbose**]

- *ipv6-address* - The IPv6 address of the device to ping. The address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- *host-name* - The name the IPv6 device to ping. A host name can be resolved into an IPv6 address using DNS.
- *datagram-size* - Specifies the size of the datagram to send in each ping. (Range: 48 - 18024 bytes)
- *repeat-count* - The number of pings to send. (Range: 1 - 2147483647)
- *hex-data-pattern* - The data pattern to send. (Range: 0 - FFFF)
- *source-address* - The source address or name to include in the ping. This is normally set to an address assigned to the interface sending the ping.
- *seconds* - The timeout interval. (Range: 0 to 3600 seconds)
- **verbose** - Displays detailed output.

Default Setting

repeat - 5
timeout - 2 seconds

Command Mode

Normal Exec - The only command options are *count* and *size*.
Privileged Exec - All command options are available.

Command Usage

- Ping sends an echo request to the specified address, and waits for a reply. Ping output can help determine path reliability, path delays, and if the host is reachable or functioning.
- If the system cannot map an address for a host name, it returns the message “Can not get address information for host,” or “protocol not running.”
- To terminate a ping session, type the escape sequence Ctrl-X.
- Using a timeout of zero seconds generates a flood ping, resulting in replies that are received only from immediately adjacent routers (depending on the utilization on the both the target and intermediate devices), the distance to the remote device, and other factors.
- Not all protocols require hosts to support pings. For some protocols, only another switch or router of the same type may respond to ping requests.
- Use the IPv4 **ping** command (page 41-6) for addresses that resolve to IPv4.

Example

```
Console# ping ipv6 2001:0DB8::3/64 repeat 5

Which outside interface [1]:1
Type ESC to abort.
Sending 5, [100]-byte ICMP Echos to 2009:DB9:2229::80, timeout is 2 seconds.
!!!!!
Success rate is 100 percent
round-trip min/max/avg = 10/30/14.000000 ms
Console#
```

Related Commands

ping (41-6)

ipv6 neighbor

This command configures a static entry in the IPv6 neighbor discovery cache. Use the **no** form to remove a static entry from the cache.

Syntax

ipv6 neighbor *ipv6-address* **vlan** *vlan-id hardware-address*
no ipv6 mtu

- *ipv6-address* - The IPv6 address of a neighbor device that can be reached through one of the network interfaces configured on this router. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- *vlan-id* - VLAN ID (Range: 1-4093)
- *hardware-address* - The 48-bit MAC layer address for the neighbor device. This address must be formatted as six hexadecimal pairs separated by hyphens.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Address Resolution Protocol (ARP) has been replaced in IPv6 with the Neighbor Discovery Protocol (NDP). The **ipv6 neighbor** command is similar to the **mac-address-table static** command (page 31-1) that is implemented using ARP.
- Static entries can only be configured on an IPv6-enabled interface.
- The router does not determine whether a static entry is reachable before placing it in the IPv6 neighbor discovery cache.
- If the specified entry was dynamically learned through the IPv6 neighbor discovery process, and already exists in the neighbor discovery cache, it is converted to a static entry. Static entries in the IPv6 neighbor discovery cache are not modified if subsequently detected by the neighbor discovery process.
- Disabling IPv6 on an interface with the **no ipv6 enable** command (see page 41-7) deletes all dynamically learned entries in the IPv6 neighbor discovery cache for that interface, but does not delete static entries.

Example

The following maps a static entry for global unicast address to a MAC address:

```
Console(config)#ipv6 neighbor 2009:DB9:2229::81  vlan 1 30-65-14-01-11-86
Console(config)#end
Console#show ipv6 neighbors
IPv6 Address                 Age           Link-layer Addr     State        Vlan
2009:DB9:2229::80            956           12-34-11-11-43-21   STALE        1
2009:DB9:2229::81            Permanent     30-65-14-01-11-86   REACH        1
FE80::1034:11FF:FE11:4321    961           12-34-11-11-43-21   STALE        1
Console#
```

Related Commands

show ipv6 neighbors (41-30)
mac-address-table static (31-1)

ipv6 nd dad attempts

This command configures the number of consecutive neighbor solicitation messages sent on an interface during duplicate address detection. Use the **no** form to restore the default setting.

Syntax

ipv6 nd dad attempts *count*
no ipv6 nd dad attempts

count - The number of neighbor solicitation messages sent to determine whether or not a duplicate address exists on this interface. (Range: 0-600)

Default Setting

1

Command Mode

Interface Configuration (VLAN)

Command Usage

- Configuring a value of 0 disables duplicate address detection.
- Duplicate address detection determines if a new unicast IPv6 address already exists on the network before it is assigned to an interface.
- Duplicate address detection is stopped on any interface that has been suspended (see the **vlan** command on page 34-6). While an interface is suspended, all unicast IPv6 addresses assigned to that interface are placed in a “pending” state. Duplicate address detection is automatically restarted when the interface is administratively re-activated.
- An interface that is re-activated restarts duplicate address detection for all unicast IPv6 addresses on the interface. While duplicate address detection is performed on the interface’s link-local address, the other IPv6 addresses remain in a “tentative” state. If no duplicate link-local address is found, duplicate address detection is started for the remaining IPv6 addresses.
- If a duplicate address is detected, it is set to “duplicate” state, and a warning message is sent to the console. If a duplicate link-local address is detected, IPv6 processes are disabled on the interface. If a duplicate global unicast address is detected, it is not used. All configuration commands associated with a duplicate address remain configured while the address is in “duplicate” state.
- If the link-local address for an interface is changed, duplicate address detection is performed on the new link-local address, but not for any of the IPv6 global unicast addresses already associated with the interface.

Example

The following configures five neighbor solicitation attempts for addresses configured on VLAN 1. The **show ipv6 interface** command indicates that the duplicate address detection process is still on-going.

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd dad attempts 5
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is stalled.
Link-local address:
  FE80::200:E8FF:FE90:0/64 [TENTATIVE]
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64 [TENTATIVE]
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
Console#
```

Related Commands

ipv6 nd ns interval (41-29)
show ipv6 neighbors (41-30)

ipv6 nd ns interval

This command configures the interval between transmitting IPv6 neighbor solicitation messages on an interface. Use the **no** form to restore the default value.

Syntax

ipv6 nd ns-interval *milliseconds*
no ipv6 nd ns-interval

milliseconds - The interval between transmitting IPv6 neighbor solicitation messages. (Range: 1000-3600000)

Default Setting

- 1000 milliseconds is used for neighbor discovery operations
- 0 milliseconds is advertised in router advertisements

Command Mode

Interface Configuration (VLAN)

Command Usage

- When a non-default value is configured, the specified interval is used both for router advertisements and by the router itself.
- This command specifies the interval between transmitting neighbor solicitation messages when resolving an address, or when probing the

reachability of a neighbor. Therefore, avoid using very short intervals for normal IPv6 operations.

Example

The following sets the interval between sending neighbor solicitation messages to 30000 milliseconds:

```
Console(config)#interface vlan 1
Console(config-if)#ipv6 nd ns-interval 30000
Console(config-if)#end
Console#show ipv6 interface
Vlan 1 is up
IPv6 is enable.
Link-local address:
  FE80::200:E8FF:FE90:0/64
Global unicast address(es):
  2009:DB9:2229::79, subnet is 2009:DB9:2229:0::/64
Joined group address(es):
  FF01::1/16
  FF02::1/16
  FF02::1:FF00:79/104
  FF02::1:FF90:0/104
MTU is 1500 bytes.
ND DAD is enabled, number of DAD attempts: 5.
ND retransmit interval is 1000 milliseconds
ND router advertisements are sent every 200 seconds
Console#
```

Related Commands

show running-config (23-5)

show ipv6 neighbors

This command displays information in the IPv6 neighbor discovery cache.

Syntax

show ipv6 neighbors [**vlan** *vlan-id* | *ipv6-address*]

- *vlan-id* - VLAN ID (Range: 1-4093)
- *ipv6-address* - The IPv6 address of a neighbor device. You can specify either a link-local or global unicast address formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.

Default Setting

All IPv6 neighbor discovery cache entries are displayed.

Command Mode

Normal Exec - No command options are available.
Privileged Exec - All command options are available.

Example

The following shows all known IPv6 neighbors for this router:

```
Console#show ipv6 neighbors
IPv6 Address                  Age        Link-layer Addr     State       Vlan
2009:DB9:2229::79             666        00-00-E8-90-00-00   STALE       1
FE80::200:E8FF:FE90:0         671        00-00-E8-90-00-00   STALE       1
Console#
```

Table 41-6 show ipv6 neighbors - display description

Field	Description
IPv6 Address	IPv6 address of neighbor
Age	The time since the address was verified as reachable (in minutes). A static entry is indicated by the value “Permanent.”
Link-layer Addr	Physical layer MAC address.
State	The following states are used for dynamic entries: • INCMP (Incomplete) - Address resolution is being carried out on the entry. A neighbor solicitation message has been sent to the multicast address of the target, but it has not yet returned a neighbor advertisement message. • REACH (Reachable) - Positive confirmation was received within the last ReachableTime interval that the forward path to the neighbor was functioning. While in REACH state, the device takes no special action when sending packets. • STALE - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. While in STALE state, the device takes no action until a packet is sent. • DELAY - More than the ReachableTime interval has elapsed since the last positive confirmation was received that the forward path was functioning. A packet was sent within the last DELAY_FIRST_PROBE_TIME interval. If no reachability confirmation is received within this interval after entering the DELAY state, the router will send a neighbor solicitation message and change the state to PROBE. • PROBE - A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer interval until confirmation of reachability is received. • ???? - Unknown state. The following states are used for static entries: • INCMP (Incomplete)-The interface for this entry is down. • REACH (Reachable) - The interface for this entry is up. Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache.
VLAN	VLAN interface from which the address was reached.

Related Commands

show mac-address-table (31-3)

clear ipv6 neighbors

This command deletes all dynamic entries in the IPv6 neighbor discovery cache.

Command Mode

Privileged Exec

Example

The following deletes all dynamic entries in the IPv6 neighbor cache:

```
Console#clear ipv6 neighbors
Console#
```

Address Resolution Protocol (ARP)

This section describes commands used to configure ARP on the switch.

Table 41-7 Address Resolution Protocol Commands

Command	Function	Mode	Page
arp	Adds a static entry in the ARP cache	GC	41-32
arp timeout	Sets the time a dynamic entry remains in the ARP cache	GC	41-33
clear arp-cache	Deletes all dynamic entries from the ARP cache	PE	41-34
show arp	Displays entries in the ARP cache	NE, PE	41-34
ip proxy-arp	Enables proxy ARP service	VC	41-35

arp

This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

Syntax

arp *ip-address hardware-address*
no arp *ip-address*

- *ip-address* - IP address to map to a specified hardware address.
- *hardware-address* - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

Default Setting

No default entries

Command Mode

Global Configuration

Command Usage

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (i.e., Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is 128.

- You may need to enter a static entry in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

Related Commands

clear arp-cache
show arp

arp timeout

This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default.

Syntax

arp-timeout *seconds*
no arp-timeout

seconds - The time a dynamic entry remains in the ARP cache. (Range: 300-86400; 86400 is one day)

Default Setting

1200 seconds (20 minutes)

Command Mode

Global Configuration

Command Usage

- When a ARP entry expires, it is deleted from the cache and an ARP request packet is sent to re-establish the MAC address.
- The aging time determines how long dynamic entries remain in the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.
- Use the **show arp** command (page 41-34) to display the current cache timeout value.

Example

This example sets the ARP cache timeout for 15 minutes (i.e., 900 seconds).

```
Console(config)#arp timeout 900
Console(config)#
```

clear arp-cache

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

Command Mode

Privileged Exec

Example

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

show arp

This command displays entries in the Address Resolution Protocol (ARP) cache.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type “other” indicates local addresses for this router.

Example

This example displays all entries in the ARP cache.

```
Console#show arp
Arp cache timeout: 1200 (seconds)

    IP Address       MAC Address        Type    Interface
--------------- ----------------- --------- -----------
       10.1.0.0 ff-ff-ff-ff-ff-ff      other          1
     10.1.0.254 00-00-ab-cd-00-00      other          1
     10.1.0.255 ff-ff-ff-ff-ff-ff      other          1
  123.20.10.123 02-10-20-30-40-50       static        2
   345.30.20.23 09-50-40-30-20-10     dynamic         3

Total entry : 5
Console#
```

ip proxy-arp

This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

Syntax

[**no**] **ip proxy-arp**

Default Setting

Disabled

Command Mode

Interface Configuration (VLAN)

Command Usage

- Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.
- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Example

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

Chapter 42: IP Routing Commands

After you configure network interfaces for this router, you must set the paths used to send traffic between different interfaces. If you enable routing on this device, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the router to the enterprise network.

Table 42-1 IP Routing Commands

Command Group	Function	Page
Global Routing Configuration	Configures global parameters for static and dynamic routing, displays the routing table, and statistics for protocols used to exchange routing information	42-1
Routing Information Protocol (RIP)	Configures global and interface specific parameters for RIP	42-5
Open Shortest Path First (OSPF)	Configures global and interface specific parameters for OSPF	42-18

Global Routing Configuration

Table 42-2 Global Routing Configuration Commands

Command	Function	Mode	Page
ip routing	Enables static and dynamic IP routing	GC	42-1
ip route	Configures static routes	GC	42-2
clear ip route	Deletes specified entries from the routing table	PE	42-3
show ip route	Displays specified entries in the routing table	PE	42-3
show ip host-route	Displays displays the interface associated with known routes	PE	42-4
show ip traffic	Displays statistics for IP, ICMP, UDP, TCP and ARP protocols	PE	42-5

ip routing

This command enables IP routing. Use the **no** form to disable IP routing.

Syntax

[**no**] **ip routing**

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- The command affects both static and dynamic unicast routing.
- If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing via RIP or OSPF, and other packets for all non-IP protocols (e.g., NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

Example

```
Console(config)#ip routing
Console(config)#
```

ip route

This command configures static routes. Use the **no** form to remove static routes.

Syntax

ip route {*destination-ip netmask* | **default**} {*gateway*} [**metric** *metric*]
no ip route {*destination-ip netmask* | **default** | *****}

- *destination-ip* – IP address of the destination network, subnetwork, or host.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **default** – Sets this entry as the default route.
- *gateway* – IP address of the gateway used for this route.
- *metric* – Selected RIP cost for this interface. (Range: 1-5, default: 1)
- ***** – Removes all static routing table entries.

Default Setting

No static routes are configured.

Command Mode

Global Configuration

Command Usage

- You can configure up to 64K static routes.
- If a static route is defined, it will always take preference over a dynamic route.
- Static routes are included in RIP and OSPF updates periodically sent by the router if this feature is enabled by the RIP or OSPF **redistribute** command (see page 42-11 or page 42-25, respectively).

Example

This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

clear ip route

This command removes dynamically learned entries from the IP routing table.

Syntax

clear ip route {*network* [*netmask*] | *****}

- *network* – Network or subnet address.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ***** – Removes all dynamic routing table entries.

Command Mode

Privileged Exec

Command Usage

- This command only clears dynamically learned routes.
- Use the **no ip address** command to remove a local interface.
- Use the **no ip route** command to remove a static route.

Example

```
Console#clear ip route 10.1.5.0
Console#
```

show ip route

This command displays information in the IP routing table.

Syntax

show ip route [**config** | *address* [*netmask*]]

- **config** – Displays all static routing entries.
- *address* – IP address of the destination network, subnetwork or host for which routing information is to be displayed.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

Command Mode

Privileged Exec

Command Usage

If the *address* is specified without the *netmask* parameter, the router displays all routes for the corresponding natural class address (page 42-9).

Example

```
Console#show ip route

  Ip Address        Netmask         Next Hop       Protocol  Metric Interface
--------------- --------------- --------------- ---------- ------ ---------
        0.0.0.0         0.0.0.0     10.2.48.102     static      0         1
      10.2.48.2   255.255.252.0      10.2.48.16      local      0         1
       10.2.5.6   255.255.255.0       10.2.8.12        RIP      1         2
       10.3.9.1   255.255.255.0      10.2.9.254 OSPF-intra      2         3


Total entry: 4
Console#
```

Table 42-3 show ip route - display description

Field	Description
Ip Address	IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.
Netmask	Network mask for the associated IP subnet.
Next Hop	IP address of the next hop (or gateway) used for this route.
Protocol	The protocol which generated this route information. (Values: static, local, RIP, OSPF)
Metric	Cost for this interface.
Interface	VLAN interface through which this address can be reached.

show ip host-route

This command displays the interface associated with known routes.

Command Mode

Privileged Exec

Example

```
Console#show ip host-route
Total count: 0
  IP address                Mac address           VLAN     Port
  --------------------     --------------------   ------   ------
  192.168.   1.250         00-00-30-01-01-01         3     1/ 1
   10.   2. 48.   2        00-00-30-01-01-02         1     1/ 1
   10.   2.   5.   6       00-00-30-01-01-03         1     1/ 2
   10.   3.   9.   1       00-00-30-01-01-04         2     1/ 3

Console#
```

Table 42-4 show ip host-route - display description

Field	Description
Ip address	IP address of the destination network, subnetwork, or host.
Mac address	The physical layer address associated with the IP address.
VLAN	The VLAN that connects to this IP address.
Port	The port that connects to this IP address.

show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

Command Mode

Privileged Exec

Command Usage

For a description of the information shown by this command, see “Displaying Statistics for IP Protocols” on page 19-16.

Example

```
Console#show ip traffic
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:   9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#
```

Routing Information Protocol (RIP)

This section describes commands used to configure RIP global and interface parameters for dynamic routing on the switch.

Table 42-5 Routing Information Protocol Commands

Command	Function	Mode	Page
router rip	Enables the RIP routing protocol	GC	42-6
default-metric	Sets the default metric assigned to external routes imported from other protocols	RC	42-7
timers basic	Sets basic timers, including update, timeout, garbage collection	RC	42-8
network	Specifies the network interfaces that are to use RIP routing	RC	42-9
neighbor	Defines a neighboring router with which to exchange information	RC	42-9

Table 42-5 Routing Information Protocol Commands (Continued)

Command	Function	Mode	Page
version	Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command)	RC	42-11
redistribute	Redistribute routes from one routing domain to another	RC	42-11
ip rip receive version	Sets the RIP receive version to use on a network interface	IC	42-12
ip rip send version	Sets the RIP send version to use on a network interface	IC	42-13
ip split-horizon	Enables split-horizon or poison-reverse loop prevention	IC	42-14
ip rip authentication key	Enables authentication for RIP2 packets and specifies keys	IC	42-14
ip rip authentication mode	Specifies the type of authentication used for RIP2 packets	IC	42-15
show rip globals	Displays global configuration settings and statistics for RIP	PE	42-16
show ip rip	Displays RIP configuration information for each network interface	PE	42-16

router rip

This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router. Use the **no** form to disable it.

Syntax

[**no**] **router rip**

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

Example

```
Console(config)#router rip
Console(config-router)#
```

Related Commands

network (42-9)

default-metric

This command sets the default metric assigned to external routes imported from other protocols. Use the **no** form to restore the default value.

Syntax

default-metric *metric-value*
no default-metric

metric-value – Metric assigned to external routes. (Range: 0-15)

Command Mode

Router Configuration

Default Setting

8

Command Usage

- This command does not override the metric value set by the **redistribute** command (see page 42-11). When a metric value has not been configured by the **redistribute** command, the **default-metric** command sets the metric value to be used for all imported external routes.
- The default metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, note that using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

Example

This example sets the default metric to 5.

```
Console(config-router)#default-metric 5
Console(config-router)#
```

Related Commands

redistribute (42-11)

timers basic

This command configures the RIP update timer, timeout timer, and garbage-collection timer. Use the **no** form to restore the defaults.

Syntax

timers basic *update-seconds*
no timers basic

update-seconds – Sets the update timer to the specified value, sets the timeout time value to 6 times the update time, and sets the garbage-collection timer to 4 times the update time.
(Range for update timer: 15-60 seconds)

Command Mode

Router Configuration

Default Setting

Update: 30 seconds
Timeout: 180 seconds
Garbage collection: 120 seconds

Command Usage

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (i.e., the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging it.
- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.
- These timers must be set to the same values for all routers in the network.

Example

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

network

This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

Syntax

[**no**] **network** *subnet-address*

subnet-address – IP address of a network directly connected to this router.

Command Mode

Router Configuration

Default Setting

No networks are specified.

Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:

  0 - 127 is class A, and only the first field in the network address is used.
  128 - 191 is class B, and the first two fields in the network address are used.
  192 - 223 is class C, and the first three fields in the network address are used.

Example

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

Related Commands

router rip (42-6)

neighbor

This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

Syntax

[**no**] **neighbor** *ip-address*

ip-address - IP address to map to a specified hardware address.

Command Mode

Router Configuration

Default Setting

No neighbors are defined.

Command Usage

This command can be used to configure a static neighbor with which this router will exchange information, rather than relying on broadcast messages generated by the RIP protocol.

Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

version

This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

Syntax

version {**1** | **2**}
no version

- **1** - RIP Version 1
- **2** - RIP Version 2

Command Mode

Router Configuration

Default Setting

RIP Version 2

Command Usage

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the following values:
  - RIP Version 1 configures the unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures the unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the default send or receive version.

Example

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

Related Commands

ip rip receive version (42-12)
ip rip send version (42-13)

redistribute

This command imports external routing information from other routing domains (that is, protocols or static routes) into the autonomous system. Use the **no** form to disable this feature.

Syntax

[**no**] **redistribute** (**ospf** | **static**} [**metric** <*metric-value*>]

- **ospf** - External routes will be imported from the Open Shortest Path First (OSPF) protocol into this routing domain.
- **static** - Static routes will be imported into this routing domain.
- *metric-value* - Metric value assigned to all external routes for the specified protocol. (Range: 1-15)

Command Mode

Router Configuration

Default Setting

redistribution - none:

metric-value - set by the **default-metric** command (see page 42-7)

Command Usage

- When a metric value has not been configured by the **redistribute** command, the **default-metric** command (page 42-7) sets the metric value to be used for all imported external routes.
- A route metric must be used to resolve the problem of redistributing external routes with incompatible metrics.
- It is advisable to use a low metric when redistributing routes from another protocol into RIP. Using a high metric limits the usefulness of external routes redistributed into RIP. For example, if a metric of 10 is defined for redistributed routes, these routes can only be advertised to routers up to 5 hops away, at which point the metric exceeds the maximum hop count of 15. By defining a low metric of 1, traffic can follow a imported route the maximum number of hops allowed within a RIP domain. However, using a low metric can increase the possibility of routing loops For example, this can occur if there are multiple redistribution points and the router learns about the same external network with a better metric from a redistribution point other than that derived from the original source.

Example

This example redistributes routes learned from OSPF and sets the metric for all external routes imported from OSPF to a value of 3.

```
Console(config-router)#redistribute ospf metric 3
Console(config-router)#
```

This example redistributes static routes and sets the metric for all of these routes to a value of 3.

```
Console(config-router)#redistribute static metric 3
Console(config-router)#
```

Related Commands

default-metric (42-7)

ip rip receive version

This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

Syntax

ip rip receive version {**none** | **1** | **2** | **1 2**}
no ip rip receive version

- **none** - Does not accept incoming RIP packets.
- **1** - Accepts only RIPv1 packets.
- **2** - Accepts only RIPv2 packets.
- **1 2** - Accepts RIPv1 or RIPv2 packets

Command Mode

Interface Configuration (VLAN)

Default Setting

1 2 (RIPv1 or RIPv2 packets)

Command Usage

- Use this command to override the global setting specified by the RIP **redistribute** command.
- You can specify the receive version based on these options:
  - Use “none” if you do not want to add any dynamic entries to the routing table for an interface. (For example, you may only want to allow static routes for a specific interface.)
  - Use “1” or “2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “1 2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

Example

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

Related Commands

redistribute (42-11)

ip rip send version

This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

Syntax

ip rip send version {**none** | **1** | **2** | **v2-broadcast**}
no ip rip send version

- **none** - Does not transmit RIP updates.
- **1** - Sends only RIPv1 packets.
- **2** - Sends only RIPv2 packets.
- **v2-broadcast** - Route information is broadcast to other routers with RIPv2.

Command Mode

Interface Configuration (VLAN)

Default Setting

v2-broadcast (RIPv1 compatible)

Command Usage

- Use this command to override the global setting specified by the RIP **redistribute** command.
- You can specify the receive version based on these options:
  - Use “none” to passively monitor route information advertised by other routers attached to the network.
  - Use “1” or “2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use “v2-broadcast” to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)

Example

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

Related Commands

redistribute (42-11)

ip split-horizon

This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable split-horizon.

Syntax

ip split-horizon [**poison-reverse**]
no ip split-horizon

poison-reverse - Enables poison-reverse on the current interface.

Command Mode

Interface Configuration (VLAN)

Default Setting

split-horizon

Command Usage

- Split horizon never propagates routes back to an interface from which they have been acquired.
- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)

Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```

ip rip authentication key

This command enables authentication for RIPv2 packets and specifies the key that must be used on an interface. Use the **no** form to prevent authentication.

Syntax

ip rip authentication key *key-string*
no ip rip authentication

key-string - A password used for authentication.
(Range: 1-16 characters, case sensitive)

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)

- For authentication to function properly, both the sending and receiving interface must be configured with the same password.

Example

This example sets an authentication password of “small” to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication key small
Console(config-if)#
```

Related Commands

ip rip authentication mode (42-15)

ip rip authentication mode

This command specifies the type of authentication that can be used on an interface. Note that the current firmware version only supports a simple password. Use the **no** form to restore the default value.

Syntax

ip rip authentication mode {**text** | **md5**}
no ip rip authentication mode

- **text** - Indicates that a simple password will be used.
- **md5** - Message Digest 5 (MD5) authentication

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- The password to be used for authentication is specified in the **ip rip authentication key** command (page 42-14).
- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.
- MD5 is a one-way hash algorithm is that takes the authentication key and produces a 128 bit message digest or “fingerprint.” This makes it computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.

Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

Related Commands

ip rip authentication key (42-14)

show rip globals

This command displays global configuration settings for RIP.

Command Mode

Privileged Exec

Example

```
Console#show rip globals

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 0
Number of Queries: 1
Console#
```

Table 42-6 show rip globals - display description

Field	Description
RIP Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.

show ip rip

This command displays information about interfaces configured for RIP.

Syntax

show ip rip {**configuration** | **status** | **peer**}

- **configuration** - Shows RIP configuration settings for each interface.
- **status** - Shows the status of routing messages on each interface.
- **peer** - Shows information on neighboring routers, along with information about the last time a route update was received, the RIP version used by the neighbor, and the status of routing messages received from this neighbor.

Command Mode

Privileged Exec

Example

```
Console#show ip rip configuration

     Interface      SendMode       ReceiveMode     Poison       Authentication
--------------- --------------- -------------- -------------- ------------------
     10.1.0.253   rip1Compatible    RIPv1Orv2   SplitHorizon   noAuthentication
     10.1.1.253   rip1Compatible    RIPv1Orv2   SplitHorizon   noAuthentication
Console#show ip rip status

     Interface   RcvBadPackets   RcvBadRoutes      SendUpdates
--------------- --------------- -------------- ---------------
     10.1.0.253               0              0              13
     10.1.1.253               0              0              13
Console#show ip rip peer

          Peer    UpdateTime   Version   RcvBadPackets   RcvBadRoutes
--------------- ------------ --------- --------------- --------------
     10.1.0.254         1625         2               0              0
     10.1.1.254         1625         2               0              0
Console#
```

Table 42-7   show ip rip - display description

Field	Description
show ip rip configuration	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, or RIPv2-broadcast)
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1 or RIPv2)
Poison	Shows if split-horizon, poison-reverse, or no protocol message loopback prevention method is in use.
Authentication	Shows if authentication is set to simple password, MD5, or none.
show ip rip status	
Interface	IP address of the interface.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
show ip rip peer	
Peer	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Open Shortest Path First (OSPF)

This section describes commands used to configure OSPF global and interface parameters for dynamic routing on the switch.

Table 42-8 Open Shortest Path First Commands

Command	Function	Mode	Page
General Configuration			
router ospf	Enables the OSPF routing protocol and enters OSPF configuration mode	GC	42-19
router-id	Sets the router ID for this device	RC	42-20
compatible rfc1583	Calculates summary route costs using RFC 1583 (OSPFv2)	RC	42-20
default-information originate	Generates a default external route into an autonomous system	RC	42-21
timers spf	Configures the hold time between consecutive SPF calculations	RC	42-22
Route Metrics and Summaries			
area range	Summarizes routes advertised by an ABR	RC	42-23
area default-cost	Sets the cost for a default summary route sent into a stub or NSSA	RC	42-24
summary-address	Summarizes routes advertised by an ASBR	RC	42-24
redistribute	Redistribute routes from one routing domain to another	RC	42-25
Area Configuration			
network area	Assigns specified interface to an area	RC	42-26
area stub	Defines a stubby area that cannot send or receive LSAs	RC	42-27
area nssa	Defines a not-so-stubby that can import external routes	RC	42-28
area virtual-link	Defines a virtual link from an area border routers to the backbone	RC	42-30
Interface Configuration			
ip ospf authentication	Specifies the authentication type for an interface	IC	42-32
ip ospf authentication-key	Assigns a simple password to be used by neighboring routers	IC	42-33
ip ospf message-digest-key	Enables MD5 authentication and sets the key for an interface	IC	42-34
ip ospf cost	Specifies the cost of sending a packet on an interface	IC	42-35
ip ospf dead-interval	Sets the interval at which he lo packets are not seen before neighbors declare the router down	IC	42-36
ip ospf hello-interval	Specifies the interval between sending hello packets	IC	42-36
ip ospf priority	Sets the router priority used to determine the designated router	IC	42-37
ip ospf retransmit-interval	Specifies the time between resending a link-state advertisement	IC	42-38
ip ospf transmit-delay	Estimates time to send a link-state update packet over an interface	IC	42-38

Table 42-8 Open Shortest Path First Commands (Continued)

Command	Function	Mode	Page
Display Information			
show ip ospf	Displays general information about the routing processes	PE	42-39
show ip ospf border-routers	Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR)	PE	42-40
show ip ospf database	Shows information about different LSAs in the database	PE	42-41
show ip ospf interface	Displays interface information	PE	42-49
show ip ospf neighbor	Displays neighbor information	PE	42-50
show ip ospf summary-address	Displays all summary address redistribution information	PE	42-51
show ip ospf virtual-links	Displays parameters and the adjacency state of virtual links	PE	42-51

router ospf

This command enables Open Shortest Path First (OSPF) routing for all IP interfaces on the router and enters router configuration mode. Use the **no** form to disable OSPF.

Syntax

[**no**] **router ospf**

Command Mode

Global Configuration

Default Setting

Disabled

Command Usage

OSPF is used to specify how routers exchange routing table information.

Example

```
Console(config)#router ospf
Console(config-router)#
```

Related Commands

network area (42-26)

router-id

This command assigns a unique router ID for this device within the autonomous system. Use the **no** form to use the default router identification method (i.e., the lowest interface address).

Syntax

router-id *ip-address*
no router-id

ip-address - Router ID formatted as an IP address.

Command Mode

Router Configuration

Default Setting

Lowest interface address

Command Usage

- The router ID must be unique for every router in the autonomous system. Using the default setting based on the lowest interface address ensures that each router ID is unique. Also, note that the router ID you cannot be set to 0.0.0.0 or 255.255.255.255.
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** (page 42-19) followed by the **router ospf** command.
- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

Example

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

Related Commands

router ospf (42-19)

compatible rfc1583

This command calculates summary route costs using RFC 1583 (early OSPFv2). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

Syntax

[**no**] **compatible rfc1583**

Command Mode

Router Configuration

Default Setting

RFC 1583 compatible

Command Usage

- When RFC 1583 compatibility is enabled, only cost is used when choosing among multiple AS-external LSAs advertising the same destination. When disabled, preference is based on type of path, using cost only to break ties (see RFC 2328).
- All routers in an OSPF routing domain should use the same RFC for calculating summary routes.
- If there are any OSPF routers in an area exchanging summary information (specifically, ABRs) which have not been upgraded to OSPFv2, this command should be used on the newly upgraded OSPFv2 routers to ensure compatibility with routers still running older OSPFv2 code. Once all systems have been upgraded to newer OSPFv2 code, use the no form of this command to restore compatibility for all systems with RFC 2328.

Example

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

default-information originate

This command generates a default external route into an autonomous system. Use the **no** form to disable this feature.

Syntax

default-information originate [**always**] [**metric** *interface-metric*] [**metric-type** *metric-type*]

no default-information originate

- **always** - Always advertise a default route to the local AS regardless of whether the router has a default route. (See “ip route” on page 42-2.)
- *interface-metric* - Metric assigned to the default route. (Range: 1-65535; Default: 10)
- *metric-type* - External link type used to advertise the default route. (Options: Type 1, Type 2; Default: Type 2)

Command Mode

Router Configuration

Default Setting

Disabled
Metric: 10 (with always option), 1 (without always option)
Metric Type: 2

Command Usage

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.
- When you use this command to redistribute routes into a routing domain (i.e., an Autonomous System, this router automatically becomes an Autonomous

System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.

  - If you use the **always** keyword, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. (To define a default route, use the **ip route** command.)
  - If you do *not* use the **always** keyword, the router can only advertise a default external route into the AS if the **redistribute** command is used to import external routes via RIP or static routing, and such a route is known.

- Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

Example

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20
metric-type 2
Console(config-router)#
```

Related Commands

ip route (42-2)
redistribute (42-25)

timers spf

This command configures the hold time between making two consecutive shortest path first (SPF) calculations. Use the **no** form to restore the default value.

Syntax

timers spf *spf-holdtime*
no timers spf

spf-holdtime - Minimum time between two consecutive SPF calculations. (Range: 0-65535 seconds)

Command Mode

Router Configuration

Default Setting

10 seconds

Command Usage

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

Example

```
Console(config-router)#timers spf 20
Console(config-router)#
```

area range

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

Syntax

[**no**] **area** *area-id* **range** *ip-address netmask* [**advertise** | **not-advertise**]

- *area-id* - Identifies an area for which the routes are summarized. (The area ID must be in the form of an IPv4 address.)
- *ip-address* - Base address for the routes to summarize.
- *netmask* - Network mask for the summary route.
- **advertise** - Advertises the specified address range.
- **not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- This command can be used to summarize intra-area routes and advertise this information to other areas through Area Border Routers (ABRs).
- If the network addresses within an area are assigned in a contiguous manner, the ABRs can advertise a summary route that covers all of the individual networks within the area that fall into the specified range using a single area range command.
- If routes are set to be advertised, the router will issue a Type 3 summary LSA for each address range specified with this command.
- This router supports up 64 summary routes for area ranges.

Example

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0 advertise
Console(config-router)#
```

area default-cost

This command specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

Syntax

area *area-id* **default-cost** *cost*
no area *area-id* **default-cost**

- *area-id* - Identifier for a stub or NSSA, in the form of an IPv4 address.
- *cost* - Cost for the default summary route sent to a stub or NSSA. (Range: 0-16777215)

Command Mode

Router Configuration

Default Setting

1

Command Usage

- Use this option only on an area border router attached to a stub area or NSSA.
- If the default cost is set to “0,” the router will not advertise a default route into the attached stub or NSSA.

Example

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

Related Commands

area stub (42-27)

summary-address

This command aggregates routes learned from other protocols. Use the **no** form to remove a summary address.

Syntax

[**no**] **summary-address** *summary-address netmask*

- *summary-address* - Summary address covering a range of addresses.
- *netmask* - Network mask for the summary route.

Command Mode

Router Configuration

Default Setting

No summary routes are defined.

Command Usage

- Redistributing routes from other protocols into OSPF normally requires the router to advertise each route individually in an external LSA. An Autonomous System Boundary Router (ASBR) can be configured to redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems. This helps both to decrease the number of external LSAs and the size of the OSPF link state database.
- This router supports up 16 Type-5 summary routes.

Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

Related Commands

area range (42-23)
redistribute (42-25)

redistribute

This command redistributes external routing information from other routing protocols and static routes into an autonomous system. Use the no form to disable this feature or to restore the default settings.

Syntax

[**no**] **redistribute** {**rip** | **static**} [**metric** *metric-value*] [**metric-type** *type-value*]

- **rip** - Imports entries learned through the Routing Information Protocol into this Autonomous System.
- **static** - Imports static routes into this Autonomous System.
- *metric-value* - Metric assigned to all external routes for the specified protocol. (Range: 1-65535: Default: 10)
- *type-value*
  - **1** - Type 1 external route
  - **2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

Command Mode

Router Configuration

Default Setting

redistribution - none
protocol - RIP and static
metric-value - 0
type-metric - 2

Command Usage

- This command is used to import routes learned from other routing protocols into the OSPF domain, and to generate AS-external-LSAs.
- When external routes are redistributed into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the **default-information originate** command to generate a “default” external route into the AS, the metric value specified in this command supersedes the metric specified in the **default-information originate** command.
- Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. When a Type 1 LSA is received by a router, it adds the internal cost to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. When a Type 2 LSA is received by a router, it only uses the external route metric to determine route cost.

Example

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

Related Commands

default-information originate (42-21)

network area

This command defines an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interfaces.

Syntax

[**no**] **network** *ip-address netmask* **area** *area-id*

- *ip-address* - Interfaces with addresses that fall within the network address are added to the operational OSPF area.
- *netmask* - Network mask of the address range to add to the area.
- *area-id* - Area to which the matching interfaces are assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IPv4 address.)

Command Mode

Router Configuration

Default Setting

Disabled

Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router (which is not already part of the backbone) must be connected to the backbone via a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- Be sure to include the primary address for an interface in the network area, otherwise, OSPF will not operate for any secondary addresses covered by the command.
- An interface can only be assigned to a single area. If an address range is overlapped in subsequent network area commands, the router will implement the address range for the area specified in the last command, and ignore the overlapping ranges in subsequent commands. However, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.
- If an address range is overlapped in subsequent network area commands, the router will use the network area with the address range that most closely matches the interface address. Also, note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.
- This router supports up to 64 OSPF router interfaces, and up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To alter the summary attribute, use the **no** form with the summary or no-summary keyword.

Syntax

[**no**] **area** *area-id* **stub** [**summary** | **no-summary**]

- *area-id* - Identifies the stub area.
  (The area ID must be in the form of an IPv4 address.)
- **summary** - Makes an Area Border Router (ABR) send a summary link advertisement into the stub area.
- **no-summary** - Stops an Area Border Router (ABR) from sending a summary link advertisement into the stub area.

Command Mode

Router Configuration

Default Setting

No stub is configured.
Summary advertisement are sent into the stub.

Command Usage

- All routers in a stub must be configured with the same area ID using this command.
- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The no-summary option can be used to completely isolate the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- Use the no-summary parameter of this command on the ABR attached to the stub to define a totally stubby area. Define an area as a totally stubby area only if routers in the area do not require summary LSAs from other areas.
- Use the **area default-cost** command to specify the cost of a default summary route sent into a stub by an ABR.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

Related Commands

area default-cost (42-24)

area nssa

This command defines a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

Syntax

[**no**] **area** *area-id* **nssa** [**no-redistribution**] [**default-information-originate**]

- *area-id* - Identifies the NSSA.
  (The area ID must be in the form of an IPv4 address.)
- **no-redistribution** - Use this keyword when the router is an NSSA Area Border Router (ABR) and the **redistribute** command is required to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned via routers in other areas) into the NSSA.

- **default-information-originate** - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate a Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

Command Mode

Router Configuration

Default Setting

No NSSA is configured.

Command Usage

- There are no external routes in an OSPF stub area, so routes cannot be redistributed from another protocol into a stub area. On the other hand, an NSSA allows external routes from another protocol to be redistributed into its own area, and then leaked to adjacent areas.
- This command can be used to simplify administration when connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as an NSSA.
- All routers in a NSSA must be configured with the same area ID.
- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default-information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.
- External routes advertised into an NSSA can include network destinations outside the AS learned via OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Example

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa default-information-originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

Syntax

[**no**] **area** *area-id* **virtual-link** *router-id*
[**authentication-key** *key*] | [**message-digest-key** *key-id* **md5** *key*]

[**no**] **area** *area-id* **virtual-link** *router-id*
authentication [**message-digest** | **null**]
[**authentication-key**] | [**message-digest-key md5**]

[**no**] **area** *area-id* **virtual-link** *router-id*
[**authentication**] [**dead-interval** *seconds*] [**hello-interval** *seconds*]
[**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

- *area-id* - Identifies the transit area for the virtual link. (The area ID must be in the form of an IPv4 address.)
- *router-id* - Router ID of the virtual link neighbor. This specifies the Area Border Router (ABR) at the other end of the virtual link. To create a virtual link, enter this command for an ABR at both ends of the link. One of the ABRs must be next to the isolated area and the transit area at one end of the link, while the other ABR must be next to the transit area and backbone at the other end of the link.
- **authentication-key** *key* - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (i.e., autonomous system). This key is only used when authentication is enabled for the backbone.
- **message-digest-key** *key-id* **md5** *key* - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 1-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.
- **authentication** - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.
  - **message-digest** - Specifies message-digest (MD5) authentication.
  - **null** - Indicates that no authentication is used.
- **dead-interval** *seconds* - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be

the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)

- **hello-interval** *seconds* - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)
- **retransmit-interval** *seconds* - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)
- **transmit-delay** *seconds* - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-3600 seconds; Default: 1 seconds)

Command Mode

Router Configuration

Default Setting

area-id: None
router-id: None
hello-interval: 10 seconds
retransmit-interval: 5 seconds
transmit-delay: 1 second
dead-interval: 40 seconds
authentication-key: None
message-digest-key: None

Command Usage

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it not possible to physically connect an area to the backbone, a virtual link can be used. A virtual link can provide a logical path to the backbone for an isolated area, or can be configured as a backup connection that can take over if the normal connection to the backbone fails. You can specify up to 32 virtual links on this router.
- A virtual link can be configured between any two backbone routers that have an interface to a common non-backbone area. The two routers joined by a virtual link are treated as if they were connected by an unnumbered point-to-point network.
- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.
- This router supports up 64 virtual links.

Example

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

Related Commands

show ip ospf virtual-links (42-51)

ip ospf authentication

This command specifies the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

Syntax

ip ospf authentication [**message-digest** | **null**]
no ip ospf authentication

- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.

Command Mode

Interface Configuration (VLAN)

Default Setting

No authentication

Command Usage

- Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key. All neighboring routers on the same network with the same password will exchange routing data.
- This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces.
- When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
- When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the

authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the pre-specified target message digest.

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- The plain-text authentication-key, or the MD5 key-id and key, must be used consistently throughout the autonomous system.

Example

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

Related Commands

ip ospf authentication-key (42-33)
ip ospf message-digest-key (42-34)

ip ospf authentication-key

This command assigns a simple password to be used by neighboring routers to verify the authenticity of routing protocol messages. Use the **no** form to remove the password.

Syntax

ip ospf authentication-key *key*
no ip ospf authentication-key

key - Sets a plain text password. (Range: 1-8 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

No password

Command Usage

- Before specifying plain-text password authentication for an interface with the **ip ospf authentication** command, configure a password with this command.
- This command creates a password (key) that is inserted into the OSPF header when routing protocol packets are originated by this device. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password will exchange routing data.
- A different password can be assigned to each network interface basis, but the password must be used consistently on all neighboring routers throughout a network (i.e., autonomous system).

Example

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

Related Commands

ip ospf authentication (42-32)

ip ospf message-digest-key

This command enables message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

Syntax

ip ospf message-digest-key *key-id* **md5** *key*
no ip ospf message-digest-key *key-id*

- *key-id* - Index number of an MD5 key. (Range: 1-255)
- *key* - Alphanumeric password used to generate a 128 bit message digest or “fingerprint.” (Range: 1-16 characters)

Command Mode

Interface Configuration (VLAN)

Default Setting

MD5 authentication is disabled.

Command Usage

- Before specifying MD5 authentication for an interface with the **ip ospf authentication** command, configure the message-digest key-id and key with this command.
- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Example

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

Related Commands

ip ospf authentication (42-32)

ip ospf cost

This command explicitly sets the cost of sending a packet on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf cost *cost*
no ip ospf cost

cost - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

- The interface cost indicates the overhead required to send packets across a certain interface. This is advertised as the link cost in router link state advertisements.
- Routes are assigned a metric equal to the sum of all metrics for each interface link in the route.
- Interface cost reflects the port speed. This router uses a default cost of 1 for all ports. Therefore, if you install a 10 Gigabit module, you may have to reset the cost for all of the 100 Mbps ports to a value greater than 1.
- This router uses a default cost of 1 for all interfaces. Therefore, if any of the interfaces used operate at 10 Gbps or greater (when using trunking), the cost for all 1000 Mbps ports should be reset using this command to a value greater than 1 to reflect the actual interface bandwidth.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

ip ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

Syntax

ip ospf dead-interval *seconds*
no ip ospf dead-interval

seconds - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

40, or four times the interval specified by the **ip ospf hello-interval** command.

Command Usage

The dead-interval is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

Related Commands

ip ospf hello-interval (42-36)

ip ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

Syntax

ip ospf hello-interval *seconds*
no ip ospf hello-interval

seconds - Interval at which hello packets are sent from an interface. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

10 seconds

Command Usage

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

ip ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for a network segment. Use the **no** form to restore the default value.

Syntax

ip ospf priority *priority*
no ip ospf priority

priority - Sets the interface priority for this router. (Range: 0-255)

Command Mode

Interface Configuration (VLAN)

Default Setting

1

Command Usage

- A designated router (DR) and backup designated router (BDR) are elected for each OSPF network segment based on Router Priority. The DR forms an active adjacency to all other routers in the network segment to exchange routing topology information. If for any reason the DR fails, the BDR takes over this role.
- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- Configure router priority for multi-access networks only and not for point-to-point networks.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

ip ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

Syntax

ip ospf retransmit-interval *seconds*
no ip ospf retransmit-interval

seconds - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

5 seconds

Command Usage

- A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
- Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

ip ospf transmit-delay

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

Syntax

ip ospf transmit-delay *seconds*
no ip ospf transmit-delay

seconds - Sets the estimated time required to send a link-state update. (Range: 1-65535)

Command Mode

Interface Configuration (VLAN)

Default Setting

1 second

Command Usage

- LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links.
- If this delay is not added, the time required to transmit an LSA over the link is not taken into consideration by the routing process. On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.

Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

show ip ospf

This command shows basic information about the routing configuration.

Command Mode

Privileged Exec

Example

```
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
     rip with metric mapped to 10
Number of area in this router is 2
Area 0.0.0.0 (BACKBONE)
     Number of interfaces in this area is 1
     SPF algorithm executed 19 times
Area 10.1.0.0
     Number of interfaces in this area is 4
     SPF algorithm executed 19 times
Console#
```

Table 42-9 show ip ospf - display description

Field	Description
Routing Process with ID	Router ID
Supports only single TOS (TOS0) route	Type of service is not supported, so you can only assign one cost per interface
It is an *router type*	The types displayed include internal, area border, or autonomous system boundary routers
Number of areas in this router	The number of configured areas
Area *identifier*	The area address, and area type if backbone, NSSA or stub

Table 42-9 show ip ospf - display description (Continued)

Field	Description
Number of interfaces	The number of interfaces attached to this area
SPF algorithm executed	The number of times the shortest path first algorithm has been executed for this area

show ip ospf border-routers

This command shows entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

Command Mode

Privileged Exec

Example

```
Console#show ip ospf border-routers

  Destination      Next Hop      Cost   Type  RteType      Area         SPF No
--------------- --------------- ------ ----- -------- --------------- -------
     10.1.1.252      10.1.1.253      0   ABR    INTRA        10.1.0.0       3
     10.2.6.252      10.2.9.253      0   ASBR   INTER        10.2.0.0       7
Console#
```

Table 42-10 show ip ospf border-routers - display description

Field	Description
Destination	Identifier for the destination router
Next Hop	IP address of the next hop toward the destination
Cost	Link metric for this route
Type	Router type of the destination; either ABR, ASBR or both
RteType	Route type; either intra-area or interarea route (INTRA or INTER)
Area	The area from which this route was learned
SPF No	The number of times the shortest path first algorithm has been executed for this route

show ip ospf database

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

Syntax

show ip ospf [*area-id*] **database** [**adv-router** [*ip-address*]]

show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**asbr-summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**database-summary**]

show ip ospf [*area-id*] **database** [**external**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**external**] [*link-state-id*] [**self-originate**] [*ip-address*]

show ip ospf [*area-id*] **database** [**network**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**network**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**nssa-external**] [*link-state-id*] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**router**] [*link-state-id*]
show ip ospf [*area-id*] **database** [[**router**] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**router**] [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**self-originate**] [*link-state-id*]

show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*]
show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**adv-router** [*ip-address*]]
show ip ospf [*area-id*] **database** [**summary**] [*link-state-id*] [**self-originate**] [*link-state-id*]

- *area-id* - Area defined for which you want to view LSA information. (This item must be entered in the form of an IP address.)
- **adv-router** - IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- *ip-address* - IP address of the specified router. If no address is entered, information about the local router is displayed.
- **asbr-summary** - Shows information about Autonomous System Boundary Router summary LSAs.
- *link-state-id* - The network portion described by an LSA. The *link-state-id* entered should be:
  - An IP network number for Type 3 Summary and External LSAs
  - A Router ID for Router, Network, and Type 4 AS Summary LSAs

  Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).
- **self-originate** - Shows LSAs originated by this router.
- **database-summary** - Shows a count for each LSA type for each area stored in the database, and the total number of LSAs in the database.
- **external** - Shows information about external LSAs.
- **network** - Shows information about network LSAs.
- **nssa-external** - Shows information about NSSA external LSAs.
- **router** - Shows information about router LSAs.
- **summary** - Shows information about summary LSAs.

Command Mode

Privileged Exec

Examples

The following shows output for the **show ip ospf database** command.

```
Console#show ip ospf database


     Displaying Router Link States(Area 10.1.0.0)
       Link ID      ADV Router    Age      Seq#     Checksum
--------------- --------------- ------ ----------- -----------
     10.1.1.252      10.1.1.252     26  0X80000005      0X89A1
     10.1.1.253      10.1.1.253     23  0X80000002      0X8D9D


     Displaying Net Link States(Area 10.1.0.0)
       Link ID      ADV Router    Age      Seq#     Checksum
--------------- --------------- ------ ----------- -----------
     10.1.1.252      10.1.1.252     28  0X80000001      0X53E1
Console#
```

Table 42-11 show ip ospf database - display description

Field	Description
Link ID	Router ID
ADV Router	Advertising router ID
Age	Age of LSA (in seconds)
Seq#	Sequence number of LSA (used to detect older duplicate LSAs)
Checksum	Checksum of the complete contents of the LSA

The following shows output when using the **asbr-summary** keyword.

```
Console#show ip ospf database asbr-summary

OSPF Router with id(10.1.1.253)

          Displaying Summary ASB Link States(Area 0.0.0.0)


LS age: 433
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 192.168.5.1 (AS Boundary Router's Router ID)
Advertising Router: 192.168.1.5
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0
Metric: 1

Console#
```

Table 42-12   show ip ospf asbr-summary - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to AS boundary routers
Link State ID	Interface address of the autonomous system boundary router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metrics	Cost of the link

The following shows output when using the **database-summary** keyword.

```
Console#show ip ospf database database-summary


Area ID (10.1.0.0)
       Router    Network    Sum-Net    Sum-ASBR    External-AS      External-Nssa
          2         1          1          0             0               0
Total LSA Counts : 4
Console#
```

Table 42-13 show ip ospf database-summary - display description

Field	Description
Area ID	Area identifier
Router	Number of router LSAs
Network	Number of network LSAs
Sum-Net	Number of summary LSAs
Sum-ASBR	Number of summary ASBR LSAs
External-AS	Number of autonomous system external LSAs
External-Nssa	Number of NSSA external network LSAs
Total LSA Counts	Total number of LSAs

The following shows output when using the **external** keyword.

```
Console#show ip ospf database external

OSPF Router with id(192.168.5.1) (Autonomous system 5)

          Displaying AS External Link States


LS age: 433
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.1.1.253 (External Network Number)
Advertising Router: 10.1.2.254
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0

Console#
```

Table 42-14 show ip ospf external - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS)
Link State ID	IP network number (External Network Number)
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Metric Type	Type 1 or Type 2 external metric (see “redistribute” on page 42-25)
Metrics	Cost of the link
Forward Address	Forwarding address for data to be passed to the advertised destination (If set to 0.0.0.0, data is forwarded to the originator of the advertisement)
External Route Tag	32-bit field attached to each external route (Not used by OSPF; may be used to communicate other information between boundary routers as defined by specific applications)

The following shows output when using the **network** keyword.

```
Console#show ip ospf database network

OSPF Router with id(10.1.1.253)

          Displaying Net Link States(Area 10.1.0.0)


Link State Data Network (Type 2)
-------------------------------

LS age: 433
Options: Support External routing capability
LS Type: Network Links
Link State ID: 10.1.1.252 (IP interface address of the Designated Router)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0

       Attached Router: 10.1.1.252
       Attached Router: 10.1.1.253
Console#
```

Table 42-15 show ip ospf network - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Network Link - LSA describes the routers attached to the network
Link State ID	Interface address of the designated router
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Address mask for the network
Attached Router	List of routers attached to the network; i.e., fully adjacent to the designated router, including the designated router itself

The following shows output when using the **router** keyword.

```
Console#show ip ospf database router

OSPF Router with id(10.1.1.253)

          Displaying Router Link States(Area 10.1.0.0)


Link State Data Router (Type 1)
-------------------------------

LS age: 233
Options: Support External routing capability
LS Type: Router Links
Link State ID: 10.1.1.252 (Originating Router's Router ID)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000011
LS Checksum: 0x7287
Length: 48
Router Role: Area Border Router
Number of Links: 1
-------------------------------------------------------
Link ID:  10.1.7.0 (IP Network/Subnet Number)
   Link Data: 255.255.255.0 (Network's IP address mask)
   Link Type: Connection to a stub network
   Number of TOS metrics: 0
   Metrics: 1

Console#
```

Table 42-16   show ip ospf router - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Router Link - LSA describes the router's interfaces.
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Router Role	Description of router type, including: None, AS Boundary Router, Area Border Router, or Virtual Link
Number of Links	Number of links described by the LSA
Link ID	Link type and corresponding Router ID or network address
Link Data	• Router ID for transit network • Network's IP address mask for stub network • Neighbor Router ID for virtual link
Link Type	Link-state type, including transit network, stub network, or virtual link

Table 42-16 show ip ospf router - display description (Continued)

Field	Description
Number of TOS metrics	Type of Service metric – This router only supports TOS 0 (or normal service)
Metrics	Cost of the link

The following shows output when using the **summary** keyword.

```
Console#show ip ospf database summary

OSPF Router with id(10.1.1.253)

          Displaying Summary Net Link States(Area 10.1.0.0)


Link State Data Summary (Type 3)
-------------------------------

LS age: 686
Options: Support External routing capability
LS Type: Summary Links(Network)
Link State ID: 10.2.6.0 (The destination Summary Network Number)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000003
LS Checksum: 0x3D02
Length: 28
Network Mask: 255.255.255.0
Metric: 1

Console#
```

Table 42-17 show ip ospf summary - display description

Field	Description
OSPF Router id	Router ID
LS age	Age of LSA (in seconds)
Options	Optional capabilities associated with the LSA
LS Type	Summary Links - LSA describes routes to networks
Link State ID	Router ID of the router that originated the LSA
Advertising Router	Advertising router ID
LS Sequence Number	Sequence number of LSA (used to detect older duplicate LSAs)
LS Checksum	Checksum of the complete contents of the LSA
Length	The length of the LSA in bytes
Network Mask	Destination network’s IP address mask
Metrics	Cost of the link

show ip ospf interface

This command displays summary information for OSPF interfaces.

Syntax

show ip ospf interface [**vlan** *vlan-id*]

vlan-id - VLAN ID (Range: 1-4093)

Command Mode

Privileged Exec

Example

```
Console#show ip ospf interface vlan 1

Vlan 1 is up
  Interface Address 10.1.1.253, Mask 255.255.255.0, Area 10.1.0.0
  Router ID 10.1.1.253, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router id 10.1.1.252, Interface address 10.1.1.252
  Backup Designated router id 10.1.1.253, Interface addr 10.1.1.253
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Console#
```

Table 42-18 show ip ospf interface - display description

Field	Description
Vlan	VLAN ID and Status of physical link
Interface Address	IP address of OSPF interface
Mask	Network mask for interface address
Area	OSPF area to which this interface belongs
Router ID	Router ID
Network Type	Includes broadcast, non-broadcast, or point-to-point networks
Cost	Interface transmit cost
Transmit Delay	Interface transmit delay (in seconds)
State	• Disabled – OSPF not enabled on this interface • Down – OSPF is enabled on this interface, but interface is down • Loopback – This is a loopback interface • Waiting – Router is trying to find the DR and BDR • DR – Designated Router • BDR – Backup Designated Router • DRother – Interface is on a multiaccess network, but is not the DR or BDR
Priority	Router priority
Designated Router	Designated router ID and respective interface address
Backup Designated Router	Backup designated router ID and respective interface address
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

show ip ospf neighbor

This command displays information about neighboring routers on each interface within an OSPF area.

Syntax

show ip ospf neighbor

Command Mode

Privileged Exec

Example

```
Console#show ip ospf neighbor

      ID           Pri        State           Address
--------------- ------ ---------------- ---------------
     10.1.1.252      1           FULL/DR        10.1.1.252

Console#
```

Table 42-19 show ip ospf neighbor - display description

Field	Description
ID	Neighbor’s router ID
Pri	Neighbor’s router priority
State	OSPF state and identification flag States include: Down – Connection down Attempt – Connection down, but attempting contact (for non-broadcast networks) Init – Have received Hello packet, but communications not yet established Two-way – Bidirectional communications established ExStart – Initializing adjacency between neighbors Exchange – Database descriptions being exchanged Loading – LSA databases being exchanged Full – Neighboring routers now fully adjacent Identification flags include: D – Dynamic neighbor S – Static neighbor DR – Designated router BDR – Backup designated router
Address	IP address of this interface

show ip ospf summary-address

This command displays all summary address information.

Syntax

show ip ospf summary-address

Command Mode

Privileged Exec

Example

This example shows a summary address and associated network mask.

```
Console#show ip ospf summary-address
10.1.0.0/255.255.0.0
Console#
```

Related Commands

summary-address (42-24)

show ip ospf virtual-links

This command displays detailed information about virtual links.

Syntax

show ip ospf virtual-links

Command Mode

Privileged Exec

Example

```
Console#show ip ospf virtual-links
Virtual Link to router 10.1.1.253 is up
Transit area 10.1.1.0
Transmit Delay is 1 sec
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Console#
```

Table 42-20 show ip ospf virtual-links - display description

Field	Description
Virtual Link to router	OSPF neighbor and link state (up or down)
Transit area	Common area the virtual link crosses to reach the target router
Transmit Delay	Estimated transmit delay (in seconds) on the virtual link
Timer intervals	Configuration settings for timer intervals, including Hello, Dead and Retransmit

Related Commands

area virtual-link (42-30)

Section IV:Appendices

This section provides additional information on the following topics.

Appendix A: Software Specifications

Software Features

Authentication
Local, RADIUS, TACACS+, Port (802.1X), HTTPS, SSH, Port Security

Access Control Lists
256 ACLs (96 MAC rules, 96 IP rules, 96 IPv6 rules)

DHCP Client, Relay, Server

BOOTP Client

DNS Client, Proxy

Port Configuration
1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex
1000BASE-SX/LX/LH - 1000 Mbps at full duplex (SFP),
10GBASE-SR/LR/ER - 10 Gbps at full duplex (Module)
10GBASE-T - 10 Gbps,1000 Mbps, 100 Mbps at full duplex (Module)

Flow Control
Full Duplex: IEEE 802.3x
Half Duplex: Back pressure

Broadcast Storm Control
Traffic throttled above a critical threshold

Port Mirroring
Multiple source ports, one destination port

Rate Limits
Input Limit
Output limit
Range (configured per port)

Port Trunking
Static trunks (Cisco EtherChannel compliant)
Dynamic trunks (Link Aggregation Control Protocol)

Spanning Tree Algorithm
Spanning Tree Protocol (STP, IEEE 802.1D-2004)
Rapid Spanning Tree Protocol (RSTP, IEEE 802.1D-2004)
Multiple Spanning Tree Protocol (MSTP, IEEE 802.1D-2004)

VLAN Support
Up to 255 groups; port-based, protocol-based, or tagged (802.1Q),
GVRP for automatic VLAN learning, private VLANs

Class of Service
Supports eight levels of priority and Weighted Round Robin Queueing
(which can be configured by VLAN tag or port),
Layer 3/4 priority mapping: IP Port, IP Precedence, IP DSCP

Quality of Service
DiffServ supports class maps, policy maps, and service policies

Multicast Filtering
IGMP Snooping

IP Routing
ARP, Proxy ARP
Static routes
RIP, RIPv2 and OSPFv2 dynamic routing
VRRP (Virtual Router Redundancy Protocol)

Additional Features
BOOTP client
CIDR (Classless Inter-Domain Routing)
SNTP (Simple Network Time Protocol)
SNMP (Simple Network Management Protocol)
RMON (Remote Monitoring, groups 1,2,3,9)
SMTP Email Alerts

Management Features

In-Band Management
Telnet, web-based HTTP or HTTPS, SNMP manager, or Secure Shell

Out-of-Band Management
RS-232 DB-9 console port

Software Loading
TFTP in-band or XModem out-of-band

SNMP
Management access via MIB database
Trap management to specified hosts

RMON
Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)

Standards

IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
Spanning Tree Protocol
Multiple Spanning Tree Protocol
Rapid Spanning Tree Protocol
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1v Protocol-based VLANs
IEEE 802.1X Port Authentication

IEEE 802.3-2005
Ethernet, Fast Ethernet, Gigabit Ethernet, and
10 Gigabit Ethernet (fiber and short-haul copper)
Link Aggregation Control Protocol (LACP)
Full-duplex flow control (ISO/IEC 8802-3)
IEEE 802.3ac VLAN tagging
IEEE 802.3an-2006 10 Gigabit Ethernet (10GBASE-T)
ARP (RFC 826)
DHCP Client (RFC 2131)
DHCP Relay (RFC 3046, 951)
DHCP Server (RFC 2131)
HTTPS
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IPv4 IGMP (RFC 3228)
OSPF (RFC 2328, 2178, 1587)
RADIUS+ (RFC 2618)
RIP (RFC 1058)
RIPv2 (RFC 2453)
RIPv2, extension (RFC 1724)
RMON (RFC 2819 groups 1,2,3,9)
SNMP (RFC 1157)
SNMPv2c (RFC 2571)
SNMPv3 (RFC DRAFT 3414, 3410, 2273, 3411, 3415)
SNTP (RFC 2030)
SSH (Version 2.0)
TFTP (RFC 1350)
VRRP (RFC 3768)

Management Information Bases

Bridge MIB (RFC 1493)
DNS Resolver MIB (RFC 1612)
Differentiated Services MIB (RFC 3289)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP MIB (RFC 2011)
IP Multicasting related MIBs
IPV6-MIB (RFC 2065)

IPV6-ICMP-MIB (RFC 2066)
IPV6-TCP-MIB (RFC 2052)
IPV6-UDP-MIB (RFC2054)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
OSPF MIB (RFC 1850)
Port Access Entity MIB (IEEE 802.1X)
Private MIB
Quality of Service MIB
RADIUS Authentication Client MIB (RFC 2621)
RIP1 MIB (RFC 1058)
RIP2 MIB (RFC 2453)
RIP2 Extension (RFC1724)
RMON MIB (RFC 2819)
RMON II Probe Configuration Group (RFC 2021, partial implementation)
SNMPv2 IP MIB (RFC 2011)
SNMP Framework MIB (RFC 3411)
SNMP-MPD MIB (RFC 3412)
SNMP Target MIB, SNMP Notification MIB (RFC 3413)
SNMP User-Based SM MIB (RFC 3414)
SNMP View Based ACM MIB (RFC 3415)
SNMP Community MIB (RFC 3584)
TACACS+ Authentication Client MIB
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)
VRRP MIB (RFC 2787)

Appendix B: Troubleshooting

Problems Accessing the Management Interface

Table B-1 Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet, web browser, or SNMP software	• Be sure the switch is powered up. • Check network cabling between the management station and the switch. • Check that you have a valid network connection to the switch and that the port you are using has not been disabled. • Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. • Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected. • If you are trying to connect to the switch via the IP address for a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. • If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Cannot connect using Secure She l	• If you cannot connect using SSH, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time. • Be sure the control parameters for the SSH server are properly configured on the switch, and that the SSH client software is properly configured on the management station. • Be sure you have generated a public key on the switch, and exported this key to the SSH client. • Be sure you have set up an account on the switch for each SSH user, including user name, authentication level, and password. • Be sure you have imported the client's public key to the switch (if public key authentication is used).
Cannot access the on-board configuration program via a serial port connection	• Be sure you have set the terminal emulator program to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps). • Check that the nu l-modem serial cable conforms to the pin-out connections provided in the Installation Guide.
Forgot or lost the password	• Contact your local distributor.

Using System Logs

If a fault does occur, refer to the Installation Guide to ensure that the problem you encountered is actually caused by the switch. If the problem appears to be caused by the switch, follow these steps:

1. Enable logging.
2. Set the error messages reported to include all categories.
3. Designate the SNMP host that is to receive the error messages.
4. Repeat the sequence of commands or other actions that lead up to the error.
5. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
6. Contact your distributor’s service engineer.

For example:

```
Console(config)#logging on
Console(config)#logging history flash 7
Console(config)#snmp-server host 192.168.1.23
⋮
```

Glossary

Access Control List (ACL)

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

Address Resolution Protocol (ARP)

ARP converts between IP addresses and MAC (i.e., hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

Boot Protocol (BOOTP)

BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

Class of Service (CoS)

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

Differentiated Services (DiffServ)

DiffServ provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

Differentiated Services Code Point Service (DSCP)

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

Domain Name Service (DNS)

A system used for translating host names for network nodes into IP addresses.

Dynamic Host Control Protocol (DHCP)

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

Extended Universal Identifier (EUI)

An address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

Extensible Authentication Protocol over LAN (EAPOL)

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP VLAN Registration Protocol (GVRP)

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

Generic Attribute Registration Protocol (GARP)

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

Generic Multicast Registration Protocol (GMRP)

GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

Group Attribute Registration Protocol (GARP)

See Generic Attribute Registration Protocol.

IEEE 802.1D

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1p

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1s

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1w

An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3ac

Defines frame extensions for VLAN tagging.

IEEE 802.3x

Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2005)

IGMP Snooping

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IGMP Query

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

Internet Control Message Protocol (ICMP)

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

Internet Group Management Protocol (IGMP)

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the “querier” and assumes responsibility for keeping track of group membership.

In-Band Management

Management of the network from a station attached directly to the network.

IP Multicast Filtering

A process whereby this switch can pass multicast traffic along to participating hosts.

IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

Layer 2

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

Layer 3

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

Link Aggregation

See Port Trunk.

Link Aggregation Control Protocol (LACP)

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

Management Information Base (MIB)

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MD5 Message-Digest Algorithm

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

Out-of-Band Management

Management of the network from a station not attached to the network.

Port Authentication

See IEEE 802.1X.

Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

Quality of Service (QoS)

QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

Remote Authentication Dial-in User Service (RADIUS)

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

Remote Monitoring (RMON)

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

Rapid Spanning Tree Protocol (RSTP)

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

Routing Information Protocol (RIP)

The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

Secure Shell (SSH)

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

Simple Mail Transfer Protocol (SMTP)

A standard host-to-host mail transport protocol that operates over TCP, port 25.

Simple Network Management Protocol (SNMP)

The application protocol in the Internet suite of protocols which offers network management services.

Simple Network Time Protocol (SNTP)

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

Spanning Tree Algorithm (STA)

A technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

Telnet

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

Terminal Access Controller Access Control System Plus (TACACS+)

TACACS+ is a logon authentication protocol that uses software running on a central server to control access to TACACS-compliant devices on the network.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

Trivial File Transfer Protocol (TFTP)

A TCP/IP protocol commonly used for software downloads.

Universal Time Coordinate (UTC)

UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth’s rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

User Datagram Protocol (UDP)

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Virtual LAN (VLAN)

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

Virtual Router Redundancy Protocol (VRRP)

A protocol that uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

XModem

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

Index

IC40240-10G
IC40480-10G